ANEXO VII - REQUISITOS DOS SERVIÇOS INTEGRADOS DE COMUNICAÇÃO

1 INTRODUÇÃO

O presente anexo descreve os requisitos técnicos relacionados à prestação de serviços de comunicação de rede WAN abrangendo roteadores, Firewalls, implantação, configuração, ambiente de Controle, gestão e monitoramento, assistência e suporte técnico dos componentes, através conectividade via circuitos MPLS, Internet Simétrica e Assimétrica, entre os Data Centers do BNB e os Postos, Parceiros, além de funcionalidades de uma Rede Definida por Software (SD-WAN) para as Unidades Distribuídas do Banco.

Os requisitos apresentados são aplicáveis, independentemente e simultaneamente, a todos os grupos de unidades descritas.

Todos os requisitos apresentados têm caráter obrigatório, devendo ser integralmente atendidos pelos licitantes de todos os ITENS, de acordo com a aplicabilidade. O não atendimento a qualquer dos requisitos apresentados, no todo ou em parte, sujeitará o licitante à desclassificação do processo licitatório, às sanções previstas em Contrato e às medidas legais cabíveis.

2 CARACTERÍSTICAS GERAIS DO SERVIÇO

2.1 Finalidade

2.1.1 Os serviços especificados neste anexo têm por finalidade a interligação entre as Unidades Distribuídas e Postos de crédito do Banco e as suas sedes localizadas em Fortaleza - CE, integrando numa mesma infraestrutura o suporte ao tráfego de dados, voz e imagens, através das tecnologias: Multiprotocol Label Switching (MPLS) e Internet.

2.1.2 Também fará parte deste anexo as especificações para interligação do Banco do Nordeste com a sua Rede Parceiros (ATP, Banco do Brasil, Caixa Econômica, Cielo e outros) através da tecnologia MPLS (somente).

2.1.3 Além do serviço de SD-WAN das Unidades Distribuídas, será contemplado no mesmo item o serviço de SSE (Security Service Edge) que deverá ser integrado com o serviço de SD-WAN, formando, assim, uma solução completa de SASE (Secure Access Service Edge). Apesar de fazerem parte do mesmo item poderão ser atendidos por fabricantes diferentes, desde que integrados e atendendo todos os itens do exigidos no edital.

2.1.4 Os serviços prestados deverão permitir a critério do Banco a criação de Tenants, sendo possível isolar a comunicação entre grupos de unidades do Banco e obrigatoriamente direcionar o tráfego entre esses grupos para dispositivos de firewall do Banco utilizando inclusive redes/VLAN diferente para rotear esse tráfego permitindo que o tráfego passe por firewall em roteamento e seja devolvido para os dispositivos de SD-WAN.

2.1.5 A critério do Banco e para cada grupo definido pelo Banco, poderá ser definido o tipo de comunicação full-mesh, parcial-mesh ou hub-to-spoke.

2.1.6 Todas as Unidades de um mesmo grupo que dispõem de tecnologia MPLS como acesso primário devem, a critério do Banco, manter comunicação ponto-a-ponto (sem passar necessariamente pelos concentradores) entre si, full-mesh, sobre o acesso primário, enquanto o acesso primário de ambas estiver ativo, independente da necessidade de subcontratação de outras provedoras pelo CONTRATADO do ITEM1

2.1.7 As Unidades de um mesmo grupo que dispõem de tecnologia MPLS como acesso secundário devem, a critério do Banco, manter comunicação ponto-a-ponto, full-mesh, sobre o acesso secundário, enquanto o acesso secundário de ambas estiver ativo,

independente da necessidade de subcontratação de outras provedoras pelo CONTRATADO do ITEM 1. Sendo que as Unidades que dispõem de tecnologia Internet Simétrica devem, a critério do Banco, manter comunicação ponto-a-ponto, VPN full-mesh, enquanto os seus acessos Internet estiverem disponíveis, independente da necessidade de subcontratação de outras provedoras pelo CONTRATADO do ITEM 1.

2.1.8 Os serviços serão providos por meio do fornecimento, para cada unidade do Banco, de um circuito de acesso primário terrestre MPLS, do acesso secundário por Internet Determinística, e outro(s) acesso(s) terciário baseado(s) em Internet Determinística ou assimétrica (incluindo o uso de tecnologia GPON) ou simétrica (incluindo EPON), de acordo com as coberturas disponíveis e todos independentes entre si; além de solução de serviços de gerenciamento e automação de circuitos WAN, com provimento de ferramentas e equipe especializada em gestão e monitoramento.

2.1.9 As Unidades denominadas Postos de crédito poderão ter os dois acessos baseados em Internet Determinística ou o primário em Internet Determinística e o secundário em Internet assimétrica.

2.1.10 A rede de parceiros será provida totalmente por links MPLS, tanto os acessos primários quanto secundários.

2.1.11 Serviços de Monitoramento e Gerenciamento das Soluções Ofertadas, inclusive NOC/SOC com recursos residentes e remotos.

2.2 Fornecimento de infraestrutura

Os serviços de circuitos de acesso a serem prestados no **ITEM 1**. deverão contemplar o fornecimento, instalação, configuração, assistência e suporte técnico de toda a infraestrutura necessária à adequada prestação dos serviços ora especificados, incluindo, além dos recursos que compõem o backbone do fornecedor dos serviços, os seguintes componentes:

2.2.1 Circuitos de acesso **primários** via MPLS terrestres para as unidades distribuídas e Parceiros, para concentração no CAPGV e no Site Secundário, englobando todos os equipamentos necessários e demais componentes relacionados. Os circuitos e acessos para as Unidades Distribuídas do Banco deverão possuir estrutura totalmente separada dos circuitos de parceiros, incluindo o acesso físico e roteadores concentradores;

2.2.2 Circuitos de acesso **secundários** via Internet Determinística Dedicada terrestre ou MPLS terrestre, dependendo da localidade. Para as Unidades Distribuídas: Internet, para os Parceiros do Banco: MPLS. Englobando todos os equipamentos e demais componentes relacionados. Os circuitos secundários e acessos para as Unidades Distribuídas do Banco, e circuito de parceiros, deverão possuir estrutura (acesso e pontos de presença – POP) totalmente separada dos circuitos primários, incluindo os acessos físicos e roteadores concentradores;

2.2.3 Circuitos de acesso **terciários** via Internet Determinística ou Assimétrica, dependendo da localidade e da cobertura, para as unidades distribuídas, englobando todos os equipamentos e demais componentes relacionados. Esses circuitos deverão possuir acessos e pontos de presença – POP totalmente separados dos circuitos primários e secundários;

2.2.4 Circuitos de acesso **primários** via Internet Determinística Dedicada terrestre para os Postos;

2.2.5 Circuitos de acesso **secundários** via Internet Determinística ou Assimétrica, dependendo da localidade e da cobertura, para os Postos , englobando todos os equipamentos e demais componentes relacionados. Esses circuitos deverão possuir acessos e pontos de presença – POP totalmente separados dos circuitos primários;

2.2.6 Caso numa determinada localidade o licitante disponha, por exemplo, de 02 (dois) Pontos de Presença (POP) com infraestruturas e acessos totalmente independentes entre si, estes poderão ser utilizados para atender até 02 (dois) links remotos, desde que realmente não compartilhem recursos, e que uma indisponibilidade ou perda de performance em um deles não afete o funcionamento e performance de ambos os links;

2.2.7 Equipamentos **roteadores** para o Site Primário, Site Secundário, Parceiros, Unidades Distribuídas (no mínimo para os circuitos primários e secundários MPLS)

2.2.8 Equipamentos **firewalls** e **Access Points** para o e Postos;

2.2.9 Os equipamentos **roteadores** a serem fornecidos no Site Primário e Site Secundário poderão ser substituídos por comutadores de rede local que implementem funcionalidades de roteamento, desde que atendidos todos os demais requisitos para os serviços ora especificados;

2.2.10 Os equipamentos **appliances** para solução de SD-WAN (*Software Defined Wide Area Network*) e seus respectivos appliances ou servidores de gerência no Site Primário, Site Secundário e Unidades Distribuídas fazem parte do escopo de atendimento do **ITEM 2**, bem como a solução de SSE (*Security Service Edge*);

2.2.11 Cabos, módulos, placas, interfaces, comutadores, memórias e demais acessórios relacionados aos componentes descritos acima (para ambos os ITENS);

2.2.12 Ao Banco, caberá providenciar a adequação das instalações físicas de suas unidades distribuídas, postos de crédito, no Site Primário e Site Secundário para proporcionar a adequada acomodação dos equipamentos fornecidos no escopo dos serviços, incluindo:

2.2.12.1 Disponibilização de espaço físico para acomodação dos equipamentos, atendendo às recomendações de refrigeração e alimentação elétrica do fabricante dos equipamentos;

2.2.12.1.1 Para a CONTRATADA do **ITEM 2**, caso os componentes ofertados a serem instalados nos datacenters ocupem espaço superior a 20 RU's (rack units), a CONTRATADA deverá entregar um rack 19 polegadas, padrão 44U, para os Sites Primário e Secundário, assim como a adequação de tubulação e encaminhamentos internos para passagem de de cabos e fibras até os racks dos núcleos/distribuição do Banco.

2.2.12.2 Adequação de tubulação e encaminhamentos internos para passagem de cabos;

2.2.12.3 Adequação do cabeamento da rede local das unidades distribuídas, postos de crédito e do CAPGV, exceto nas Unidades que dispuserem de equipamentos do tipo Access Point, em que a CONTRATADA deverá se responsabilizar pelo encaminhamento do cabeamento e fixação dos equipamentos nos locais indicados pelo Banco.

2.2.12.4 A CONTRATADA, caberá providenciar a adequação das instalações físicas externas eventuais em cada Parceiro do Banco, como, por exemplo, Golden Jump;

2.2.13 Todos os equipamentos fornecidos para a prestação dos serviços serão devidamente patrimoniados e cadastrados em sistema de inventário eletrônico atualmente utilizado pelo Banco para efeitos de controle patrimonial de bens de terceiros;

2.2.14 O Banco do Nordeste se reserva o direito de, durante a vigência do CONTRATO, realizar diligências técnicas a fim de certificar que a infraestrutura entregue pela CONTRATADA do **ITEM 1** é realmente independente nos termos deste edital. Tais diligências podem acontecer através do pedido de envio por parte do BANCO à CONTRATADA do **ITEM 1**. de plantas topográficas em formato .PDF com a

identificação fim-a-fim da infraestrutura utilizada para atender a determinada(s) unidade(s), ou através de visitas aos pontos de presença que atendem determinada(s) unidade(s), a critério do Banco. As visitas deverão ser sempre acompanhadas de técnico indicado pela CONTRATADA do **ITEM 1**, que será responsável pela correta identificação dos locais e equipamentos utilizados, a fim de demonstrar a independência dos recursos de acesso ao meio e pontos de presença das Unidades atendidas neste edital.

2.2.15 Caberá a CONTRATADA do **ITEM 1** acompanhar junto ao NOC/SOC do Banco, mesmo que de forma remota, toda a conexão/desconexão dos novos circuitos de dados com a rede do Banco, mantendo os requisitos de segurança solicitados no Edital, inclusive durante período de migração/implantação;

3 REQUISITOS PARA OS EQUIPAMENTOS (ITEM 1)

3.1 REQUISITOS GERAIS EQUIPAMENTOS ROTEADORES

Todos os equipamentos roteadores a serem fornecidos para atender os circuitos de acesso WAN primário, secundário e terciário nas Unidades Distribuídas do Banco, Parceiros, Site Primário, Site Secundário deverão atender ao seguinte conjunto de requisitos gerais:

3.1.1 Deverão ser novos, isto é, sem utilização anterior (exceto se tiverem sido utilizados com o único propósito de homologação citada neste Instrumento) e não constar em listas de end-of-support ou end-of-life do fabricante;

3.1.2 Todas as funcionalidades devem estar disponíveis na versão atual da solução ofertada, não serão aceitos equipamentos cujas funcionalidades ainda estão em desenvolvimento (Roadmap);

3.1.3 Todos os equipamentos roteadores para circuitos MPLS das Unidades Distribuídas deverão ser de um mesmo fabricante para cada localidade e incluindo os roteadores concentradores no caso de MPLS;

3.1.4 Todos os equipamentos roteadores para circuitos MPLS dos Parceiros deverão ser de um mesmo fabricante para cada localidade e incluindo os roteadores concentradores;

3.1.5 Todos os equipamentos roteadores para circuitos Internet das Unidades Distribuídas deverão ser de um mesmo fabricante para cada localidade, podendo estes serem diferentes do modelo proposto para os circuitos MPLS;

3.1.6 Todos os produtos que compõem a solução devem ser fornecidos com o devido licenciamento, incluindo licenciamento para utilização de interfaces em suas velocidades maiores, garantia de atualização de software, de manutenção e de troca do hardware/acessórios pelo período de vigência do Contrato estabelecido pelo Edital;

3.1.7 Deverá possuir LED's indicativos do estado de funcionamento do equipamento;

3.1.8 Deverá possibilitar a obtenção de estatísticas de tráfego e falhas das portas *inband* utilizadas na solução;

3.1.9 Deverão estar equipados com recursos que permitam a reconfiguração dinâmica das diversas portas e módulos utilizados na solução, inclusive permitindo a ativação e desativação de portas e módulos sem causar reinício, instabilidade ou qualquer impacto que venha a comprometer o funcionamento do equipamento;

3.1.10 Deverá possibilitar a implementação de LAN Virtual (VLAN) por porta e compatíveis com o padrão IEEE 802.1Q;

3.1.11 Deverão implementar Agregação de links (802.3ad/LACP);

3.1.12 Os equipamentos deverão implementar ajuste de clock, utilizando NTP (*Network Time Protocol*);

3.1.13 Deverão permitir as atualizações de versões de código utilizando os protocolos SFTP (SSH *File Transfer Proocol*) ou *Secure Copy Protocol* (SCP);

3.1.14 Deverão permitir enviar logs para servidores remotos (*Syslog*) (não será objeto deste certame o fornecimento de servidor para *Syslog*), onde pelo menos 1 (um) será informado pelo Banco;

3.1.15 Deverão implementar *traceroute* para o descobrimento do caminho seguido por um pacote dentro da rede;

3.1.16 Todas as portas são configuráveis MDI/MDIX, dispensando o uso de cabos *cross over* ou quaisquer configurações para conexões a outros switches;

3.1.17 Deverão implementar *Internet Protocol Flow Information eXport* (IPFIX) ou Netflow v.9 ou equivalente;

3.1.18 Todos os roteadores MPLS devem ter interfaces *loopback* dedicadas para o gerenciamento do Banco em faixa de rede especificada pelo Banco. Os acessos de gerenciamento serão realizados através dessa interface;

3.1.19 Deverão estar equipados com recursos que implementem funcionalidades de gerenciamento relativas ao padrão de gerenciamento SNMP (*Simple Network Management Protocol*), com suporte a RFC 1213 (MIB-II), suporte a SNMPv2c, Suporte ao SNMP v3 e suporte a geração de *traps*; Deverá ser fornecida uma comunidade (community) SNMP de leitura em todos os roteadores fornecidos na solução. Essa comunidade (*community*) será acessada a partir do Site Primário e Site Secundário;

3.1.20 Deverá ser capaz de apresentar estatísticas de utilização das interfaces em ambos os sentidos, entrada e saída;

3.1.21 Deverá ser fornecido usuário com acesso via SSH em todos os roteadores com permissão "somente leitura" para o BANCO, incluindo possibilidade de visualização de TODA e qualquer configuração e estatísticas de tráfego dos equipamentos para apoio no momento dos incidentes, devendo permanecer ativa durante todo o Contrato. O acesso deverá fornecer também permissão em nível de leitura para todas as estatísticas do equipamento passíveis de consulta, como QoS, estatísticas de tráfego, status de protocolos de roteamento, etc;

3.1.22 Deverão estar equipados com 1 (uma) porta de comunicação out-of-band para gerenciamento de configuração ou isolar uma porta de comunicação do roteador através de uma VLAN, tornando a porta totalmente isolada do ambiente de acesso;

3.1.23 Na implantação de cada roteador, a CONTRATADA deverá fornecer todas as gerências e requisitos conforme previsto no Edital, **Anexo X – Requisitos de Gerenciamento dos Serviços**. O não fornecimento desses acessos implicará em sanções administrativas de acordo com o **Anexo VI - Acordo de Níveis de Serviços**, além de não ser emitido o Termo de Aceitação Definitiva (TAD);

3.1.24 Deverão possuir estrutura apropriada para acondicionamento em armário de fiação (rack) de 19 polegadas, ocupando uma unidade (1U) para as remotas e até 03 (três) unidades (3U) para os concentradores;

3.1.25 Deverão implementar IPV4 e IPV6;

3.1.26 Deverá possuir ferramentas para depuração e gerenciamento em primeiro nível para IPv4 e IPv6, implementando, ao menos, testes ICMP, debug, trace e log de eventos;

3.1.27 Deverão Implementar Network Address Translation (NAT) para os principais protocolos da pilha TCP/IP;

3.1.28 Deverão implementar Jumbo Frames;

3.1.29 Deverão suportar sub-interfaces lógicas;

3.1.30 A solução deverá implementar funcionalidades de Access Control List (ACL) Simples e Estendidas;

3.1.31 Deverão possuir mecanismos de authentication, authorization and accounting (AAA) através de Servidor RADIUS e TACACS+;

3.1.32 Deverá implementar roteamento estático e dinâmico;

3.1.33 As fontes de alimentação principal deverão funcionar com tensão elétrica de 110V~220V AC, 50~60Hz, de modo automático;

3.1.34 Para cada equipamento roteador, deverão ser entregues 1 (um) cabo UTP de 2,5 metros crimpado com RJ45 de fábrica e com a devida certificação. Os mesmos deverão ser de categoria 6 ou superior. Durante ativação do roteador, os cabos deverão ter suas extremidades etiquetadas conforme padrão definido pelo Banco durante implantação.

3.1.35 A CONTRATADA deverá fornecer dois níveis de acesso ao Banco, sendo um deles somente leitura e outro com perfil administrativo para realização de configurações, quando solicitado. Ambos os acessos devem ser fornecidos para todos os equipamentos e softwares envolvidos na solução. Os acessos de leitura deverão permitir a visualização das estatísticas do equipamento passíveis de consulta, como QoS, estatísticas de tráfego, além da configuração dos equipamentos, e qualquer política criada na solução contratada. O acesso mínimo (de leitura) deverá ser fornecido acesso via HTTPS. O acesso deverá permanecer ativo durante todo o Contrato. A solução deverá implementar auditoria sobre as alterações de configuração realizadas por cada usuário. Qualquer alteração feita pelo Banco será de responsabilidade do Banco, cabendo ao CONTRATADA, monitorar e questionar sobre a configuração realizada em até 72h corridas, tornando-se a CONTRATADA responsável pela alteração na sequência para termos de SLA de disponibilidade e demais obrigações contratuais;

3.1.36 No caso de um equipamento ser compatível com acesso via SSH, será obrigatório o fornecimento do acesso ao Banco, conforme detalhado acima. Utilização de acesso de telnet (sem criptografia) para gerenciamento não será permitido no Banco;

3.1.37 O não fornecimento de quaisquer desses acessos implicará em sanções administrativas de acordo com o Anexo XI - Acordo de Níveis de Serviços, além de não ser emitido o Termo de Aceitação Definitiva (TAD);

3.2 EQUIPAMENTOS ROTEADORES <u>CONCENTRADORES</u> MPLS (Unidades Distribuídas) – EQUIPAMENTO TIPO 1

Os equipamentos roteadores concentradores MPLS que ficarão no Site Primário e Secundário serão responsáveis por receber os links concentradores MPLS das Unidades Distribuídas, além dos requisitos gerais deverão atender:

3.2.1 Deverão ser providos 02 (dois) concentradores MPLS para assumir o tráfego de MPLS das Unidades Distribuídas. Sendo 01 (um) no Site Primário e 01 (um) no Site Secundário.

3.2.2 Possuir pelo menos 04 (quatro) interfaces 1000Mbps, interfaces RJ-45, para cabos UTP categoria 6 enhanced ou superior, full duplex, GigaEthernet, auto-sense, de acordo com os protocolos padrões Ethernet IEEE 802.3 Ethernet IEEE802.3u 100BaseTX, Ethernet IEEE802.3ab 1000BaseT e IEEE802.3z 1000BASE-X, sendo duas dessas interfaces dedicadas ao fornecimento LAN para o Banco;

3.2.3 Possuir pelo menos **04 (quatro)** interfaces 10Gbps, utilizando SFP+ e conector LC para fibra do tipo multimodo padrão 10GBASE-SR entregues com line cord de 2 (dois) metros ou superior conectados, sendo as duas interfaces dedicadas ao fornecimento **LAN** para o Banco;

3.2.4 Possuir pelo menos **02 (duas)** interfaces 10Gbps compatíveis com as conexões **WAN** do provedor de serviços e seus respectivos transceivers e fibra, com line cord de 2 (dois) metros ou superior;

3.2.5 Suportar capacidade de roteamento de tráfego (throughput) mínima de **10Gbps** full duplex.

3.2.6 Deverá suportar o encaminhamento e armazenamento de pelo menos 30.000 rotas IPv4 e 10.000 rotas IPv6;

3.2.7 O fabricante dos equipamentos roteadores deverá possuir certificado de qualidade emitido pela International Standard Organization (ISO) relacionado aos processos de projeto e fabricação desses equipamentos;

3.2.8 Implementar o protocolo Virtual Redundant Router Protocol (VRRP) com monitoração de circuito e ativação automática do roteador secundário em caso de falha;

3.2.9 Implementar recurso de agregação de portas baseado no protocolo LACP;

3.2.10 Para o caso dos equipamentos que possuam a opção de adição e remoção de módulos e interfaces de rede, o mesmo deve permitir, sem a necessidade de desligamento do mesmo (mecanismo conhecido como “Hot Swap”), de permitir a troca de componentes removíveis do equipamento sem afetar a conectividade com outros circuitos que não sejam atendidos pelo componente defeituoso;

3.2.11 Implementar ICMPv6 com as seguintes funcionalidades: ICMP request; ICMP reply; ICMP Neighbor Discovery Protocol (NDP); ICMP MTU Discovery;

3.2.12 Implementar mecanismos de Dual Stack (IPv4 e IPv6);

3.2.13 Deverá implementar roteamento dinâmico RIPng e OSPFv3;

3.2.14 Deverá implementar Multiprotocol BGP (MP-BGP) com suporte a IPv6;

3.2.15 Implementar os protocolos de roteamento Open Shortest Path First (OSPF), versão 2 (compatível com RFC 1583) e BGP-4 (compatível com RFC 1771);

3.2.16 Suportar OSPF graceful restart;

3.2.17 Implementar BGP-4 (exemplo, mas não se limitando a: RFC 1771, RFC 1997, RFC 2283, RFC 2545, RFC 2858, RFC 3392, RFC 4271, RFC 4364, RFC 4456, RFC4632);

3.2.18 Implementar VRF (virtual routing and forwarding) ou similar garantindo o isolamento de tabelas de roteamento garantindo total independência do tráfego entre tabelas diferentes.

3.2.19 Deverá implementar roteamento baseado em políticas (PBR);

3.2.20 Deverá implementar roteamento baseado em uma condição de origem, inclusive dentro das VRFs;

3.2.21 Implementar Weighted Round Robin (WRR) ou Shaped Round Robin (SRR);

3.2.22 Implementar a RFC 791 Type of Service – ToS;

3.2.23 Implementar Diffserv – DS (RFCs 2474, 2475);

3.2.24 Implementar Traffic Shaping;

3.2.25 Implementar Weighted Random Early Detection (WRED) ou Weighted Tail Drop (WTD) como mecanismo de prevenção de congestionamento;

3.2.26 Deve implementar recursos que possibilite a definição de classes de serviço e alocação de banda por classes;

3.2.27 Para pacotes que excederam a especificação de banda, deve ser possível configurar pelo menos as seguintes ações:

3.2.28 Transmissão do pacote sem modificação;

3.2.29 Transmissão com remarcação do valor de DSCP;

3.2.30 Descarte do pacote;

3.2.31 Deve ser possível criar uma classe com prioridade absoluta sobre as demais dentro da quantidade de banda que lhe foi alocada;

3.2.32 Implementar classificação, marcação e priorização de tráfego com base em endereço IP de origem/destino, portas TCP/UDP de origem e destino, DSCP (Differentiated Services Code Point), precedence.

3.2.33 Implementar filtros de rotas (Prefix-list , as-path, community);

3.2.34 Implementar o protocolo de marcação de quadros (tagging) de redes locais padrão IEEE 802.1q nas interfaces utilizadas para interligação com a rede local das Unidades Distribuídas, Postos, CAPGV e Parceiros;

3.2.35 Os roteadores deverão estar instrumentalizados com funcionalidades específicas de monitoramento de níveis de serviço, compatíveis com protocolo IP-SLA ou equivalente (no mínimo: delay ICMP, delay UDP, perda de pacotes, jitter ICMP, jitter UDP) e deverão ser fornecidos privilégios de acesso de leitura para usuários designados pelo Banco para uso deste monitoramento, via SSH e software de gerenciamento do Banco;

3.2.36 Deverá possibilitar a implementação de LAN Virtual (VLAN) por porta e compatíveis com o padrão IEEE 802.1Q e IEEE 802.1Q-in-Q.

3.2.37 Possuir compatibilidade com todos os recursos técnicos solicitados para a contratação dos links MPLS.

3.2.38 Deverá implementar roteamento multicast PIM-SM (Protocol Independent ModeSparse Mode) e PIM-DM (Protocol Independent Mode-Dense Mode);

3.2.39 Deverá implementar mecanismo de controle de multicast, conforme os protocolos: IGMPv1, IGMPv2 e IGMPv3;

3.2.40 Deverá suportar o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para um endereço IP, devendo ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente;

3.2.41 Os equipamentos ofertados devem possuir fontes de 110-240V AC, redundantes e hot-swap.

3.2.42 Trabalhar em alta disponibilidade (ativo/ativo ou ativo/passivo, a critério do Banco) entre os circuitos de acesso primário e secundário;

3.2.43 No caso de interrupção dos serviços que trafegam através do circuito de acesso primário, o tráfego do serviço de dados deverá ser redirecionado para o circuito de acesso secundário, mantendo-se os requisitos mínimos especificados nos itens anteriores. O contrário também deverá ocorrer, isto é, em caso de interrupção dos serviços que trafegam no circuito secundário, o tráfego do serviço de dados deverá ser redirecionado para o circuito de acesso primário, respeitando os requisitos mínimos. Deverá implementar redundância dentro de cada Data center e entre os Data Centers também;

3.2.44 O chaveamento dos serviços entre os circuitos de acesso primário e secundário, em caso de falha do circuito primário ou secundário, deverá garantir o retorno à operação normal quando do fim da falha acontecer, em sua plenitude, de forma automática, em até 3 (três) minutos a partir do início ou fim da falha. Isso deve acontecer sem qualquer intervenção humana, quer seja para realizar configuração em equipamento ou sistema de gerência, quer seja para realizar mudanças físicas na infraestrutura fornecida;

3.2.45 Em caso de falha em um dos sites do Banco o chaveamento do tráfego deverá ocorrer entre os Sites do BANCO (Site Primário ßàSite Secundário), via roteamento dinâmico e sem intervenção manual;

3.2.46 Roteamento dinâmico IMPLEMENTADO entre os roteadores remotos e os concentradores da Rede do CAPGV. As redes publicadas no roteamento serão informadas pelo Banco durante implementação, podendo haver a necessidade de NAT em algumas comunicações. O protocolo de roteamento será definido pelo Banco durante implementação. Atualmente é utilizado BGP;

3.2.47 O(s) transceiver(s) SFP/SFP+ necessário(s) para conexão da interface dos concentradores deverão ser fornecidos em conjunto com a solução. Não será necessário o fornecimento de transceiver para o lado da conexão com a rede/equipamento do Banco;

3.3 EQUIPAMENTOS ROTEADORES REMOTOS MPLS (Unidades Distribuídas) – EQUIPAMENTO TIPO 2

Os equipamentos roteadores que serão fornecidos para as Unidades Distribuídas contempladas com acesso MPLS deverão, além dos requisitos gerais, atender:

3.3.1 Possuir pelo menos **03 (três)** interfaces 10/100/1000Mbps, interfaces RJ-45, para cabos UTP categoria 6 enhanced ou superior, full duplex, GigaEthernet, auto-sense, de acordo com os protocolos padrões Ethernet IEEE 802.3 10BaseT, Ethernet IEEE802.3u 100BaseTX, Ethernet IEEE802.3ab 1000BaseT e IEEE802.3z 1000BASE-X, exclusivas para conexão com a **LAN** do Banco**;**

3.3.2 Possuir pelo menos **01 (uma)** interfaces 1Gbps, RJ-45, compatível com a velocidade do circuito para conexão **WAN** da CONTRATADA **do ITEM 1** ;

3.3.3 Suportar capacidade de roteamento de tráfego (throughput) mínima de **1.5Gbps** full duplex.

3.3.4 As interfaces dedicadas para a LAN na rede do Banco devem ser compatíveis com conexão em modo Bridge, ou seja, com uma interface L3 (roteamento da unidade remota), que utiliza duas conexões físicas (duas interfaces), permitindo assim a conexão em diferentes appliances na rede LAN do Banco e fazendo parte do mesmo domínio de broadcast, com 1 (um) único IP (L3) para cada interface, bem como para subinterfaces (compatíveis com 802.1q);

3.3.5 Implementar roteamento estático e dinâmico para o Internet Protocol (IPv4 e IPv6);

3.3.6 Implementar ICMPv6 com as seguintes funcionalidades: ICMP request; ICMP reply; ICMP Neighbor Discovery Protocol (NDP); ICMP MTU Discovery;

3.3.7 Implementar os protocolos de roteamento Open Shortest Path First (OSPF), versão 2 (compatível com RFC 1583) e BGP-4 (compatível com RFC 1771); Ambos; os protocolos de roteamento (OSPF e BGP) devem ser também compatíveis com IPV6;

3.3.8 Suportar OSPF graceful restart;

3.3.9 Deverá implementar roteamento dinâmico RIPng e OSPFv3;

3.3.10 O roteador deverá ser capaz de fornecer IP via DHCP server para todas as Unidades Distribuídas. Dentre os parâmetros necessários, estão os endereços de DNS primário e secundário, WINS e "scope options", de acordo com solicitação do Banco. Atualmente, o Banco utiliza opções 246 e 248 com string de até 70 caracteres por exemplo. A solicitação de configuração por parte do Banco não deverá representar custos adicionais ao projeto e deverá seguir o padrão SLA;

3.3.11 Possuir função de DHCP Server, Relay e Client interno;

3.3.12 O roteador deve ser capaz de criar Interfaces VLANs L3 e realizar o roteamento dessas redes internamente na unidade remota, bem como realizar o roteamento para toda a rede do Banco;

3.3.13 O roteador deverá ser compatível com 802.1Q, no caso de subinterfaces criadas. Atualmente o Banco possui segmentação lógica para redes de videoconferência, por exemplo. A criação de novas redes não deverá representar custos adicionais ao projeto e deverá seguir o padrão SLA;

3.3.14 Deverá suportar o encaminhamento e armazenamento de pelo menos 30.000 rotas IPv4 e 10.000 rotas IPv6;

3.3.15 Implementar o protocolo Virtual Redundant Router Protocol (VRRP) com monitoração de circuito e ativação automática do roteador secundário em caso de falha;
3.3.16 Deverá implementar roteamento baseado em políticas PBR;
3.3.17 Deverá implementar roteamento baseado em uma condição de origem, inclusive dentro das VRFs;
3.3.18 Implementar recurso de agregação de portas baseado no protocolo LACP;
3.3.19 Implementar Weighted Round Robin (WRR) ou Shaped Round Robin (SRR);
3.3.20 Implementar a RFC 791 Type of Service – ToS;
3.3.21 Implementar Diffserv – DS (RFCs 2474, 2475);
3.3.22 Implementar Traffic Shaping;
3.3.23 Implementar Weighted Random Early Detection (WRED) ou Weighted Tail Drop (WTD) como mecanismo de prevenção de congestionamento;
3.3.24 Deve implementar recursos que possibilite a definição de classes de serviço e alocação de banda por classes;
3.3.25 Para pacotes que excederam a especificação de banda, deve ser possível configurar pelo menos as seguintes ações:
    3.3.25.1 Transmissão do pacote sem modificação;
    3.3.25.2 Transmissão com remarcação do valor de DSCP;
    3.3.25.3 Descarte do pacote;
3.3.26 Deve ser possível criar uma classe com prioridade absoluta sobre as demais dentro da quantidade de banda que lhe foi alocada;
3.3.27 Implementar classificação, marcação e priorização de tráfego com base em endereço IP de origem/destino, portas TCP/UDP de origem e destino, DSCP (*Differentiated Services Code Point*), precedence.
3.3.28 Implementar filtros de rotas (Prefix-list , as-path, community);
3.3.29 Implementar o protocolo de marcação de quadros (tagging) de redes locais padrão IEEE 802.1q nas interfaces 1000BaseT ethernet utilizadas para interligação com a rede local das Unidades Distribuídas, CAPGV e Parceiros;
3.3.30 Implementar Access Control List (ACL) simples e estendidas;
3.3.31 A solução deve implementar controles de políticas de acesso por IP (origem e destino) porta (destino) e protocolo, inclusive nas redes locais onde o roteador estiver conectado.
3.3.32 Deverá suportar o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para um endereço IP, devendo ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente;
3.3.33 Possuir compatibilidade com todos os recursos técnicos solicitados para a contratação dos links MPLS.
3.3.34 Os roteadores deverão estar instrumentalizados com funcionalidades específicas de monitoramento de níveis de serviço, compatíveis com protocolo IP-SLA ou equivalente (no mínimo: delay ICMP, delay UDP, perda de pacotes, jitter ICMP, jitter UDP), e deverão ser fornecidos privilégios para usuários designados pelo Banco para uso deste monitoramento, via acesso de gerência e via software de gerenciamento do Banco.

3.4 EQUIPAMENTOS ROTEADORES CONCENTRADORES DE INTERNET (Utilização pelo Banco) - EQUIPAMENTO TIPO 3

Os equipamentos roteadores concentradores que serão fornecidos para concentração Internet/Gateway, além dos requisitos gerais deverão atender:

3.4.1 Deverão ser providos 04 (quatro) concentradores INTERNET para assumir o tráfego de INTERNET das unidades distribuídas e postos de crédito. Sendo 02 (dois) no site primário e 02 (dois) no secundário;

3.4.2 Possuir pelo menos **04 (quatro)** interfaces **1000Mbps**, interfaces RJ-45, para cabos UTP categoria 6 enhanced ou superior, full duplex, GigaEthernet, auto-sense, de acordo com os protocolos padrões Ethernet IEEE 802.3 10BaseT, Ethernet IEEE802.3u 100BaseTX, Ethernet IEEE802.3ab 1000BaseT e IEEE802.3z 1000BASE-X;

3.4.3 Possuir pelo menos **08 (oito)** interfaces **10 Gbps**, com conector LC, para fibras óticas multimodo (LM), , full-duplex. Todas estas interfaces deverão ser non-blocking e deverão ser entregues com os respectivos tranceivers multimodo padrão 10GBASE-SR e com line cord de 2 (dois) metros ou superior;

3.4.4 Em caso de fornecimento de soluções com mais interfaces de conexão compatíveis com as velocidades 10/40Gbps, todas devem ser licenciadas para uso a critério do Banco e devem ser entregues com transceivers de fibra instalados. Para todas as interfaces/transceivers de fibra, deverão ser entregues fibras LC compatíveis e com tamanho de 20m mínimo.

3.4.5 Suportar capacidade de roteamento de tráfego (throughput) mínima de **20Gbps** full duplex.

3.4.6 Deverá suportar o encaminhamento e armazenamento de pelo menos **2.000.000 rotas IPv4 e 2.000.000 rotas IPv6**;

3.4.7 Trabalhar em alta disponibilidade (ativo/ativo ou ativo/passivo, a critério do Banco) entre os circuitos de acesso primário e secundário;

3.4.7.1 No caso de interrupção dos serviços que trafegam através do circuito de acesso primário, o tráfego do serviço de dados deverá ser redirecionado para o circuito de acesso secundário, mantendo-se os requisitos mínimos especificados nos itens anteriores. O contrário também deverá ocorrer, isto é, em caso de interrupção dos serviços que trafegam no circuito secundário, o tráfego do serviço de dados deverá ser redirecionado para o circuito de acesso primário, respeitando os requisitos mínimos;

3.4.7.2 Em caso de falha em um dos sites do Banco o chaveamento do tráfego deverá ocorrer entre os Sites do BANCO (Site Primário ←→ Site Secundário), via roteamento dinâmico e sem intervenção manual;

3.4.8 Roteamento dinâmico IMPLEMENTADO entre os roteadores concentradores da Rede do CAPGV. As redes publicadas no roteamento serão informadas pelo Banco durante implementação, podendo haver a necessidade de NAT em algumas comunicações. O protocolo de roteamento será definido pelo Banco durante implementação. Atualmente é BGP;

3.4.9 Suportar OSPF graceful restart;

3.4.10 Implementar ICMPv6 com as seguintes funcionalidades: ICMP request; ICMP reply; ICMP Neighbor Discovery Protocol (NDP); ICMP MTU Discovery;

3.4.11 Implementar mecanismos de Dual Stack (IPv4 e IPv6);

3.4.12 Implementar roteamento IPv6 estático e dinâmico;

3.4.13 Deverá implementar roteamento dinâmico RIPng e OSPFv3;

3.4.14 Deverá implementar Multiprotocol BGP (MP-BGP) com suporte a IPv6;

3.4.15 Implementar VRF (virtual routing and forwarding) ou similar garantindo o isolamento de tabelas de roteamento garantindo total independência do tráfego entre tabelas diferentes;

3.4.16 Implementar no mínimo 4000 VRF's (virtual routing and forwarding) ou similar;

3.4.17 Deverá implementar roteamento baseado em políticas PBR;
3.4.18 Deverá implementar roteamento baseado em uma condição de origem, inclusive dentro das VRFs;
3.4.19 Implementar os protocolos de roteamento *Open Shortest Path First* (OSPF), versão 2 (compatível com RFC 1583) e BGP-4 (compatível com RFC 1771); Ambos; os protocolos de roteamento (OSPF e BGP) devem ser também compatíveis com IPV6;
3.4.20 Implementar protocolo de roteamento dinâmico OSPF (exemplo, mas não se limitando a RFC 2328, 1587, 1765 e 2370);
3.4.21 Implementar mecanismo de segurança dos protocolos OSPF e BGP, permitindo a autenticação mútua entre peers BGP e OSPF;
3.4.22 Implementar BGP-4 (exemplo, mas não se limitando a: RFC 1771, RFC 1997, RFC 2283, RFC 2545, RFC 2858, RFC 3392, RFC 4271, RFC 4364, RFC4632);
3.4.23 Implementar BGP Route Reflection (RFC 4456);
3.4.24 Implementar o protocolo Virtual Redundant Router Protocol (VRRP) com monitoração de circuito e ativação automática do roteador secundário em caso de falha;
3.4.25 O equipamento deve possuir pelo menos 16 GB de memória RAM.
3.4.26 Implementar Weighted Round Robin (WRR) ou Shaped Round Robin (SRR);
3.4.27 Implementar a RFC 791 Type of Service – ToS;
3.4.28 Implementar Diffserv – DS (RFCs 2474, 2475);
3.4.29 Implementar Traffic Shaping;
3.4.30 Implementar Weighted Random Early Detection (WRED) ou Weighted Tail Drop (WTD) como mecanismo de prevenção de congestionamento;
3.4.31 Implementar classificação, marcação e priorização de tráfego com base em endereço IP de origem/destino, portas TCP/UDP de origem e destino, DSCP (*Differentiated Services Code Point*), precedence.
3.4.32 Implementar filtros de rotas (Prefix-list , as-path, community);
3.4.33 Implementar o protocolo de marcação de quadros (tagging) de redes locais padrão IEEE 802.1q;
3.4.34 Os roteadores deverão estar instrumentalizados com funcionalidades específicas de monitoramento de níveis de serviço, compatíveis com protocolo IP-SLA ou equivalente (no mínimo: delay ICMP, delay UDP, perda de pacotes, jitter ICMP, jitter UDP) e deverão ser fornecidos privilégios de acesso de leitura para usuários designados pelo Banco para uso deste monitoramento, via SSH e software de gerenciamento do Banco;
3.4.35 Deverá possibilitar a implementação de LAN Virtual (VLAN) por porta e compatíveis com o padrão IEEE 802.1Q e IEEE 802.1Q-in-Q.
3.4.36 No concentrador, deverão ser fornecidos equipamentos que permitam a adição e remoção de módulos e interfaces de rede sem a necessidade de desligamento do mesmo (mecanismo conhecido como “Hot Swap”), de forma a permitir a troca de componentes removíveis do equipamento sem afetar a conectividade com outros circuitos que não sejam atendidos pelo componente defeituoso;
3.4.37 Os equipamentos ofertados devem possuir fontes de 110-240V AC, redundantes e hot-swap.
3.4.38 Implementar Access Control List (ACL) simples e estendidas;
3.4.39 Implementar recurso de agregação de portas baseado no protocolo LACP;
3.4.40 Deverá implementar roteamento multicast PIM-SM (Protocol Independent ModeSparse Mode) e PIM-DM (Protocol Independent Mode-Dense Mode);
3.4.41 Deverá implementar mecanismo de controle de multicast, conforme os protocolos: IGMPv1, IGMPv2 e IGMPv3;
3.4.42 Deverá suportar o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para um endereço IP, devendo ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente;

3.4.43 Os roteadores deverão estar instrumentalizados com funcionalidades específicas de monitoramento de níveis de serviço, compatíveis com protocolo IP-SLA (sendo a função de IP-SLA source obrigatória nos roteadores concentradores) ou equivalente (no mínimo: delay ICMP, delay UDP, perda de pacotes, jitter ICMP, jitter UDP), e deverão ser fornecidos privilégios para usuários designados pelo BANCO para uso deste monitoramento

3.4.44 A estes roteadores deverá ser concedido o acesso de escrita com privilégios de administrador ao BANCO. Não será permitido à CONTRATADA **do ITEM 1** a administração desses equipamentos após aceite da Implantação. A CONTRATADA **do ITEM 1**, assim, será desobrigada a prestar gerenciamento e suporte técnico em caso de problemas de configuração ocasionados pelo BANCO. Contudo, não haverá prejuízo das obrigações da CONTRATADA **do ITEM 1** no tocante aos requisitos de assistência técnica em casos de problemas de hardware. Bem como sem prejudicar o suporte técnico no que tange ao direito de atualização de firmwares, por exemplo;

3.4.45 NÃO faz parte do escopo deste edital o provimento dos circuitos de acesso concentradores de INTERNET. Estes serão de responsabilidade do BANCO, e eventuais problemas causados por estes acessos serão abonados de quaisquer SLAs às contratadas deste certame. Atualmente o BANCO possui 4 circuitos de Internet no CAPGV, totalizando uma banda de 20Gbps.

3.5 EQUIPAMENTOS ROTEADORES REMOTOS DE INTERNET (Unidades Distribuídas)

3.5.1 O fornecimento dos equipamentos roteadores remotos de Internet para Unidades Distribuídas será facultado a CONTRATADA, podendo atender este edital sem prover equipamentos deste tipo. Sendo suficiente a entrega do acesso compatível com a velocidade determinada para a localidade e via padrão Ethernet com fornecimento de cabo UTP ethernet (categoria 6 ou superior) dentro da sala indicada pelo BANCO em cada unidade. Nesse caso, a CONTRATADA deverá ainda informar:

3.5.1.1 Endereço IP fixo;

3.5.1.2 Máscara compatível;

3.5.1.3 Default gateway.

3.5.2 Deverá permitir a integração com a Solução SD-WAN;

3.5.3 Caso a conexão Internet entregue pela CONTRATADA, necessite de algum método de autenticação e/ou discagem, NAT/PAT, etc, para o estabelecimento da comunicação, estas deverão ser feitas pelo roteador/modem entregue pela CONTRATADA, de forma que fique transparente à solução SD-WAN implantada.

3.5.4 Caso a CONTRATADA deseje fornecer os equipamentos roteadores remotos que serão fornecidos para as Unidades Distribuídas que terão acessos de Internet (Simétrica e Assimétrica), estes deverão atender:

3.5.4.1 Todos devem ser de um mesmo fabricante;

3.5.4.2 Deverão ser fornecidos e gerenciados pela operadora. O Banco deverá ter acesso às informações do equipamento relacionado ao status das interfaces, serviços disponíveis e versão de sistema operacional. O acesso deverá ser garantido via CLI, interface gráfica ou via portal de gerenciamento do provedor de serviço, desde que seja possível buscar as informações acima.

3.5.4.3 Deverão estar equipados com recursos que implementem funcionalidades de gerenciamento relativas ao padrão de gerenciamento SNMP (Simple Network

Management Protocol), com suporte a RFC 1213 (MIB-II), suporte a SNMPv2c, Suporte ao SNMP v3 e suporte a geração de traps; Deverá ser fornecida uma comunidade (community) SNMP de leitura em todos os equipamentos fornecidos na solução.

3.5.4.4 Não deverão sobre nenhuma hipótese fornecer internet via Wi-Fi, sendo obrigatório a desativação (*shutdown*) caso disponível no equipamento, e deverá ter somente uma interface ativa para conexão direta no equipamento de SD-WAN, e outra interface para conexão externa com a própria operadora. Todas as outras interfaces, se for o caso, deverão estar em shutdown. O Banco poderá a qualquer momento solicitar relatório sobre o status das portas.

3.5.4.5 Para cada equipamento deverá ser fornecido 1 (um) cabo UTP categoria 6 ou superior. Caberá a operadora a conexão do equipamento com o equipamento de SD-WAN em interface a ser especificada pelo Banco em momento de implantação, caso o equipamento SD-WAN esteja instalado antes da ativação do link de internet.

3.5.4.6 Deverão ser compatíveis com o tipo de acesso a que estão provendo: Simétrico ou Assimétrico (ADSL ou modelo de atendimento realizado via discagem PPPOE);

3.6 EQUIPAMENTOS ROTEADORES CONCENTRADORES MPLS (Parceiros)– EQUIPAMENTO TIPO 4

Os equipamentos roteadores concentradores MPLS que ficarão no Site Primário e Secundário serão responsáveis por receber os links concentradores dos links de Parceiros, além dos requisitos gerais deverão atender:

3.6.1 Deverão ser providos 04 (quatro) concentradores MPLS para assumir o tráfego de MPLS dos links de Parceiros. Sendo 02 (dois) no Site Primário e 02 (dois) no Site Secundário.

3.6.2 Possuir pelo menos 04 (quatro) interfaces 1000Mbps, interfaces RJ-45, para cabos UTP categoria 6 enhanced ou superior, full duplex, GigaEthernet, auto-sense, de acordo com os protocolos padrões Ethernet IEEE 802.3 Ethernet IEEE802.3u 100BaseTX, Ethernet IEEE802.3ab 1000BaseT e IEEE802.3z 1000BASE-X, sendo **02 (duas)** dessas interfaces dedicadas ao fornecimento **LAN** para o Banco;

3.6.3 Possuir pelo menos **02 (duas)** interfaces 10Gbps, utilizando SFP+ e conector LC para fibra do tipo multimodo padrão 10GBASE-SR entregues com line cord de 2 (dois) metros ou superior conectados, sendo as duas interfaces dedicadas ao fornecimento **LAN** para o Banco.

3.6.4 Quantidade de interfaces suficiente para receber as conexões **WAN** com o provedor de serviços,

3.6.5 Suportar capacidade de roteamento de tráfego (throughput) mínima de **4Gbps** full duplex.

3.6.6 Capacidade de concentrar as VPNs dos links remotos dos circuitos de parceiros, bem como ser responsáveis pelo roteamento e publicação de rotas dinâmicas. Caberá ao Banco definir se a comunicação será ou não via VPN (comunicação criptografada);

3.6.7 Implementar RMON (Remote Network Monitoring MIB), com suporte a RFC 2819. Deve ser permitido o acesso de leitura a pelo menos aos grupos “Statistics, History, Alarm e Events”, a partir de solução de gerência do Banco ou de empresa por ele indicado;

3.6.8 Deverá suportar o encaminhamento e armazenamento de pelo menos 30.000 rotas IPv4 e 10.000 rotas IPv6;

3.6.9 Implementar RMON (Remote Network Monitoring MIB), com suporte a RFC 2819. Deve ser permitido o acesso de leitura a pelo menos aos grupos “Statistics, History, Alarm e Events”, a partir de solução de gerência do Banco ou de empresa por ele indicado;

3.6.10 O fabricante dos equipamentos roteadores deverá possuir certificado de qualidade emitido pela International Standard Organization (ISO) relacionado aos processos de projeto e fabricação desses equipamentos;

3.6.11 Deverão ser fornecidos equipamentos que permitam a adição e remoção de módulos e interfaces de rede sem a necessidade de desligamento do mesmo (mecanismo conhecido como “Hot Swap”), de forma a permitir a troca de componentes removíveis do equipamento sem afetar a conectividade com outros circuitos que não sejam atendidos pelo componente defeituoso;

3.6.12 Implementar o protocolo Virtual Redundant Router Protocol (VRRP);

3.6.13 Implementar ICMPv6 com as seguintes funcionalidades: ICMP request; ICMP reply; ICMP Neighbor Discovery Protocol (NDP); ICMP MTU Discovery;

3.6.14 Implementar mecanismos de Dual Stack (IPv4 e IPv6);

3.6.15 Deverá implementar roteamento dinâmico RIPng e OSPFv3;

3.6.16 Deverá implementar Multiprotocol BGP (MP-BGP) com suporte a IPv6;

3.6.17 Implementar os protocolos de roteamento Open Shortest Path First (OSPF), versão 2 (compatível com RFC 1583) e BGP-4 (compatível com RFC 1771);

3.6.18 Suportar OSPF graceful restart;

3.6.19 Implementar BGP-4 (exemplo, mas não se limitando a: RFC 1771, RFC 1997, RFC 2283, RFC 2545, RFC 2858, RFC 3392, RFC 4271, RFC 4364, RFC 4456, RFC4632);

3.6.20 Implementar VRF (virtual routing and forwarding) ou similar garantindo o isolamento de tabelas de roteamento garantindo total independência do tráfego entre tabelas diferentes.

3.6.21 Deverá implementar roteamento baseado em políticas PBR;

3.6.22 Deverá implementar roteamento baseado em uma condição de origem, inclusive dentro das VRFs;

3.6.23 Implementar Weighted Round Robin (WRR) ou Shaped Round Robin (SRR);

3.6.24 Implementar a RFC 791 Type of Service – TOS;

3.6.25 Implementar Diffserv – DS (RFCs 2474, 2475);

3.6.26 Implementar Traffic Shaping;

3.6.27 Implementar Weighted Random Early Detection (WRED) ou Weighted Tail Drop (WTD) como mecanismo de prevenção de congestionamento;

3.6.28 Deve implementar recursos que possibilite a definição de classes de serviço e alocação de banda por classes;

3.6.29 Para pacotes que excederam a especificação de banda, deve ser possível configurar pelo menos as seguintes ações:

- 3.6.29.1 Transmissão do pacote sem modificação;
- 3.6.29.2 Transmissão com remarcação do valor de DSCP;
- 3.6.29.3 Descarte do pacote;

3.6.30 Deve ser possível criar uma classe com prioridade absoluta sobre as demais dentro da quantidade de banda que lhe foi alocada;

3.6.31 Implementar classificação, marcação e priorização de tráfego com base em endereço IP de origem/destino, portas TCP/UDP de origem e destino, DSCP (*Differentiated Services Code Point*), precedence.

3.6.32 Implementar filtros de rotas (Prefix-list , as-path, community);

3.6.33 Implementar mecanismos de marcação de precedência (802.1p);

3.6.34 Implementar o protocolo de marcação de quadros (tagging) de redes locais padrão IEEE 802.1q nas interfaces 1000BaseT ethernet utilizadas para interligação com a rede local das Unidades Distribuídas, CAPGV e Site Secundário;

3.6.35 Os roteadores deverão estar instrumentalizados com funcionalidades específicas de monitoramento de níveis de serviço, compatíveis com protocolo IP-SLA ou equivalente (no mínimo: delay ICMP, delay UDP, perda de pacotes, jitter ICMP, jitter UDP) e deverão ser fornecidos privilégios de acesso de leitura para usuários designados pelo Banco para uso deste monitoramento, via SSH e software de gerenciamento do Banco;

3.6.36 Deverá possibilitar a implementação de LAN Virtual (VLAN) por porta e compatíveis com o padrão IEEE 802.1Q e IEEE 802.1Q-in-Q.
3.6.37 Implementar Access Control List (ACL) simples e estendidas;
3.6.38 Implementar recurso de agregação de portas baseado no protocolo LACP;
3.6.39 Deverá implementar mecanismo de controle de multicast, conforme os protocolos: IGMPv1, IGMPv2 e IGMPv3;
3.6.40 Deverá suportar o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para um endereço IP, devendo ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente;
3.6.41 Possuir compatibilidade com todos os recursos técnicos solicitados para a contratação dos links MPLS.
3.6.42 Deverá implementar roteamento dinâmico **EIGRP** - Enhanced Interior Gateway Routing Protocol;
3.6.43 Os equipamentos ofertados devem possuir fontes de 110-240V AC, redundantes e hot-swap.
3.6.44 Trabalhar em alta disponibilidade (ativo/ativo ou ativo/passivo, a critério do Banco) entre os circuitos de acesso primário e secundário;
3.6.45 No caso de interrupção dos serviços que trafegam através do circuito de acesso primário, o tráfego do serviço de dados deverá ser redirecionado para o circuito de acesso secundário, mantendo-se os requisitos mínimos especificados nos itens anteriores. O contrário também deverá ocorrer, isto é, em caso de interrupção dos serviços que trafegam no circuito secundário, o tráfego do serviço de dados deverá ser redirecionado para o circuito de acesso primário, respeitando os requisitos mínimos;
3.6.46 O chaveamento dos serviços entre os circuitos de acesso primário e secundário de Parceiros, em caso de falha do circuito primário ou secundário, deverá garantir o retorno à operação normal quando do fim da falha acontecer, em sua plenitude, de forma automática, em até 3 (três) minutos a partir do início ou fim da falha. Isso deve acontecer sem qualquer intervenção humana, quer seja para realizar configuração em equipamento ou sistema de gerência, quer seja para realizar mudanças físicas na infraestrutura fornecida;
3.6.47 Em caso de falha em um dos sites do Banco o chaveamento do tráfego deverá ocorrer entre os Sites do BANCO (Site Primário <-> Site Secundário), via roteamento dinâmico e sem intervenção manual;
3.6.48 Roteamento dinâmico implementado na LAN do CAPGV e entre concentradores MPLS PARCEIROS e roteadores remotos MPLS PARCEIROS. As redes publicadas no roteamento serão informadas pelo Banco durante implementação, podendo haver a necessidade de NAT em algumas comunicações. O protocolo de roteamento na LAN do CAPGV será definido pelo Banco durante implementação. Atualmente é utilizado os protocolos EIGRP e BGP. O protocolo de roteamento WAN com os PARCEIROS do Banco é implementado via BGP e EIGRP.
3.6.49 O(s) transceiver(s) SFP/SFP+ necessário(s) para conexão da interface dos concentradores deverão ser fornecidos em conjunto com a solução. Não será necessário o fornecimento de transceiver para o lado da conexão com a rede/equipamento do Banco;

3.7 EQUIPAMENTOS ROTEADORES REMOTOS MPLS (Parceiros) – EQUIPAMENTO TIPO 5

Os equipamentos roteadores que serão fornecidos para os Parceiros, contemplados com acesso MPLS deverão, além dos requisitos gerais, atender:

3.7.1 Possuir pelo menos **02 (duas)** interfaces 10/100/1000Mbps, interfaces RJ-45, para cabos UTP categoria 6 enhanced ou superior, full duplex, GigaEthernet, auto-sense, de acordo

com os protocolos padrões Ethernet IEEE 802.3 10BaseT, Ethernet IEEE802.3u 100BaseTX, Ethernet IEEE802.3ab 1000BaseT e IEEE802.3z 1000BASE-X, exclusivas para conexão com a **LAN** do Banco;

3.7.2 Possuir pelo menos **01 (uma)** interfaces 1Gbps, RJ-45, compatível com a velocidade do circuito para conexão **WAN** da CONTRATADA **do ITEM 1** ;

3.7.3 Suportar capacidade de roteamento de tráfego (throughput) mínima **de 1.5Gbps full** duplex.

3.7.4 As interfaces dedicadas para a LAN na rede do Banco devem ser compatíveis com conexão em modo Bridge, ou seja, com uma interface L3 (roteamento da unidade remota), que utiliza duas conexões físicas (duas interfaces), permitindo assim a conexão em diferentes appliances na rede LAN do Banco e fazendo parte do mesmo domínio de broadcast, com 1 (um) único IP (L3) para cada interface, bem como para subinterfaces (compatíveis com 802.1q);

3.7.5 Implementar roteamento estático e dinâmico para o Internet Protocol (IP);

3.7.6 Implementar ICMPv6 com as seguintes funcionalidades: ICMP request; ICMP reply; ICMP Neighbor Discovery Protocol (NDP); ICMP MTU Discovery;

3.7.7 Implementar os protocolos de roteamento Open Shortest Path First (OSPF), versão 2 (compatível com RFC 1583) e BGP-4 (compatível com RFC 1771); Ambos; os protocolos de roteamento (OSPF e BGP) devem ser também compatíveis com IPV6;

3.7.8 Suportar OSPF graceful restart;

3.7.9 Deverá implementar roteamento dinâmico RIPng e OSPFv3;

3.7.10 O roteador deverá ser capaz de fornecer IP via DHCP server para todas as Unidades ~~Distribuídas~~. Dentre os parâmetros necessários, estão os endereços de DNS primário e secundário, WINS e "scope options", de acordo com solicitação do Banco. Atualmente, o Banco utiliza opções 246 e 248 com string de até 70 caracteres por exemplo. A solicitação de configuração por parte do Banco não deverá representar custos adicionais ao projeto e deverá seguir o padrão SLA;

3.7.11 Possuir função de DHCP Server, Relay e Client interno;

3.7.12 O roteador deve ser capaz de criar Interfaces VLANs L3 e realizar o roteamento dessas redes internamente na unidade remota, bem como realizar o roteamento para toda a rede do Banco;

3.7.13 Deverá implementar roteamento dinâmico **EIGRP** - Enhanced Interior Gateway Routing Protocol;

3.7.14 Deverá suportar o encaminhamento e armazenamento de pelo menos 30.000 rotas IPv4 e 10.000 rotas IPv6;

3.7.15 Implementar o protocolo Virtual Redundant Router Protocol (VRRP) com monitoração de circuito e ativação automática do roteador secundário em caso de falha;

3.7.16 Deverá implementar roteamento baseado em políticas PBR;

3.7.17 Deverá implementar roteamento baseado em uma condição de origem, inclusive dentro das VRFs;

3.7.18 Implementar Weighted Round Robin (WRR) ou Shaped Round Robin (SRR);

3.7.19 Implementar a RFC 791 Type of Service – ToS;

3.7.20 Implementar Diffserv – DS (RFCs 2474, 2475);

3.7.21 Implementar Traffic Shaping;

3.7.22 Implementar Weighted Random Early Detection (WRED) ou Weighted Tail Drop (WTD) como mecanismo de prevenção de congestionamento;

3.7.23 Deve implementar recursos que possibilite a definição de classes de serviço e alocação de banda por classes;

3.7.24 Para pacotes que excederam a especificação de banda, deve ser possível configurar pelo menos as seguintes ações:

3.7.24.1 Transmissão do pacote sem modificação;

3.7.24.2 Transmissão com remarcação do valor de DSCP;

3.7.24.3 Descarte do pacote;

3.7.25 Deve ser possível criar uma classe com prioridade absoluta sobre as demais dentro da quantidade de banda que lhe foi alocada;
3.7.26 Implementar classificação, marcação e priorização de tráfego com base em endereço IP de origem/destino, portas TCP/UDP de origem e destino, DSCP (*Differentiated Services Code Point*), precedence.
3.7.27 Implementar IP Precedence;
3.7.28 Implementar filtros de rotas (Prefix-list , as-path, community);
3.7.29 Deverá suportar o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para um endereço IP, devendo ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente;
3.7.30 Implementar o protocolo de marcação de quadros (tagging) de redes locais padrão IEEE 802.1q nas interfaces 1000BaseT ethernet utilizadas para interligação com a rede local;
3.7.31 Implementar Network Address Translation (NAT) para os principais protocolos da pilha TCP/IP;
3.7.32 Implementar Access Control List (ACL) simples e estendidas;
3.7.33 Implementar recurso de agregação de portas baseado no protocolo LACP;
3.7.34 Os roteadores deverão estar instrumentalizados com funcionalidades específicas de monitoramento de níveis de serviço, compatíveis com protocolo IP-SLA ou equivalente (no mínimo: delay ICMP, delay UDP, perda de pacotes, jitter ICMP, jitter UDP), e deverão ser fornecidos privilégios para usuários designados pelo Banco para uso deste monitoramento, via acesso de gerência e via software de gerenciamento do Banco.
3.7.35 Roteamento dinâmico implementado entre os roteadores concentradores da Rede MPLS. As redes publicadas no roteamento serão informadas pelo Banco durante implementação, podendo haver a necessidade de NAT em algumas comunicações. Os protocolos atualmente utilizados são BGP e EIGRP; O protocolo de roteamento WAN com os PARCEIROS do Banco é implementado via BGP e EIGRP.

3.8 Requisitos dos EQUIPAMENTOS FIREWALLS REMOTOS DO TIPO NGFW – *Next Generation Firewall* (Postos de Crédito)- EQUIPAMENTO TIPO 6

Estes equipamentos serão fornecidos para os Postos de crédito com seus circuitos Internet. A CONTRATADA deve fornecer todos os componentes de hardware, software e gerenciamento, assim como licenças requeridas e compatíveis para o seu funcionamento.

Os equipamentos serão contemplados em conjunto com acesso Internet Determinística Dedicada terrestre ou 5G (desde que garanta banda mínima dedicada, e seja ilimitada) nos circuitos primários e secundários (podendo estes últimos serem Internet Assimétrica, desde que não haja disponibilidade de Internet Determinística), nos moldes dos Postos e Unidades, e terão que atender:

Requisitos Gerais

3.8.1 Todos os firewalls devem ser de um mesmo fabricante;
3.8.2 Todos os equipamentos, produtos, peças ou produtos de software ofertados deverão ser novos e de primeiro uso (exceto se tiverem sido utilizados com o único propósito de homologação citada neste Instrumento) e não constar, no momento da apresentação da proposta, em listas de *end-of-sale, end-of-support ou end-of-life* do fabricante;

3.8.3 Todos os produtos que compõem a solução devem ser fornecidos com o devido licenciamento, incluindo garantia de atualização de software, de manutenção e de troca do hardware pelo período de vigência do Contrato estabelecido pelo Edital;

3.8.4 A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), com sistema operacional customizado/especializado, não sendo estruturado em servidores convencionais ou máquinas virtuais.

3.8.5 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, inspeção SSL, identificação de usuários e controle granular de permissões para administradores da ferramenta.

3.8.6 Deverá possuir LED's indicativos do estado de funcionamento do equipamento;

3.8.7 Deverá possibilitar a obtenção de estatísticas de tráfego e falhas das portas *inband* utilizadas na solução;

3.8.8 Deverá possibilitar a implementação de LAN Virtual (VLAN) por porta e compatíveis com o padrão IEEE 802.1Q;

3.8.9 Os equipamentos deverão implementar ajuste de clock, utilizando NTP (Network Time Protocol);

3.8.10 Deverão permitir as atualizações de versões de código utilizando os protocolos File Transfer Protocol (FTP), SFTP (SSH File Transfer Proocol) ou Trivial File Transfer Protocol (TFTP);

3.8.11 Deverão permitir enviar logs para servidores remotos (Syslog) (não será objeto deste certame o fornecimento de servidor para Syslog), onde pelo menos 1 (um) será informado pelo Banco;

3.8.12 Deverão implementar traceroute para o descobrimento do caminho seguido por um pacote dentro da rede;

3.8.13 Todas as portas são configuráveis MDI/MDIX, dispensando o uso de cabos cross over ou quaisquer configurações para conexões a outros switches;

3.8.14 Cada equipamento ofertado deve possuir, no mínimo, **02 (duas) interfaces de rede 1GbE** UTP , com funcionalidades L2/L3, para LAN do Posto.

3.8.15 Para cada equipamento entregue, deve ser entregue 2 (dois) cabos UTP de 2,5 metros crimpado com RJ45 de fábrica e com a devida certificação. O mesmo deverá ser de categoria 6 ou superior. Durante ativação do equipamento, o cabo deverá ter suas extremidades etiquetadas conforme padrão definido pelo Banco durante implantação;

3.8.16 Deverão implementar Internet Protocol Flow Information eXport (IPFIX) ou Netflow v.9 ou equivalente;

3.8.17 Possuir pelo menos **16 (dezesseis) interfaces 10/100/1000Mbps**, interfaces RJ-45, para cabos UTP categoria 6 enhanced ou superior, full duplex, GigaEthernet, auto-sense, de acordo com os protocolos padrões Ethernet IEEE 802.3 10BaseT, Ethernet IEEE802.3u 100BaseTX, Ethernet IEEE802.3ab 1000BaseT e IEEE802.3z 1000BASE-X, exclusivas para conexão com a LAN do Banco;

3.8.17.1 Será aceito o fornecimento de equipamento com menos interfaces, desde que seja fornecido em conjunto, sem custo adicional**, equipamento switch** gerenciável para complementar a quantidade de interfaces 10/100/1000Mbps RJ-45, contemplando no mínimo as mesmas *features Layer 2* das portas dos Firewalls, garantindo total compatibilidade e mesmo nível de suporte, para atender aos Postos.

3.8.18 Possuir pelo menos **02 (duas) interface RJ-45**, compatível com a velocidade do circuito, para cabos UTP categoria 6 *enhanced* ou superior, *full duplex*, GigaEthernet, auto-sense, de acordo com os protocolos padrões Ethernet IEEE 802.3 10BaseT, Ethernet IEEE802.3u 100BaseTX, *Ethernet* IEEE802.3ab 1000BaseT ou IEEE802.3z 1000BASE-X, exclusiva para conexão **WAN** da CONTRATADA;

3.8.19 Suportar endereçamento na interface WAN por pppoe (Point-to-point Protocol over ethernet), IP estático e dinâmico, por DHCP;

3.8.20 Permitir alta disponibilidade das interfaces WAN nas modalidades ativo-ativo (balanceamento) e ativo-passivo (redundância);

3.8.21 Permitir recurso de balanceamento de links WAN, com regras de balanceamento por conexão utilizando a métrica round-robin, e funcionalidade de escoamento de tráfego para a interface WAN secundária;

3.8.22 O appliance deverá ser capaz de fornecer IP via DHCP server. Dentre os parâmetros necessários, estão os endereços de DNS primário e secundário, WINS e "scope options", de acordo com solicitação do Banco. Atualmente, o Banco utiliza opções 246 e 248 com string de até 70 caracteres por exemplo. A solicitação de configuração por parte do Banco não deverá representar custos adicionais ao projeto e deverá seguir o padrão SLA;

3.8.23 Implementar *Network Address Translation* (NAT) para os principais protocolos da pilha TCP/IP;

3.8.24 A solução deverá implementar funcionalidades de Access Control List (ACL) simples e estendidas ou similar com o objetivo de permitir e/ou bloquear tráfego informados pelo Banco;

3.8.25 A CONTRATADA deste item deverá permitir a conexão de outros circuitos, a critério do BANCO, a este equipamento, desde que o BANCO se responsabilize pela contratação e gestão dos mesmos. Caberá à contratada a configuração deste equipamento para receber o novo circuito;

3.8.26 Possuir fonte de alimentação operando nas tensões 110/220V, com seleção automática de voltagem, e frequência de 50/60Hz.

3.8.27 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 (modelo OSI);

3.8.28 O software deve ser fornecido em sua versão mais atualizada.

3.8.29 Quando as funcionalidades de firewall, controle de aplicação, IPS e antivírus/antispyware estiverem habilitadas, de forma simultânea, o tráfego deve ser inspecionado de modo bidirecional, com inspeção em toda a sessão do pacote, sem qualquer utilização de recurso de bypass. Não será aceita aceleração de pacotes na placa de rede, limitando a análise somente até a camada 4, de transporte – modelo OSI.

3.8.30 O equipamento deve suportar todas as funcionalidades nativas do dispositivo de proteção, incluindo: Firewall, IPS, Antivírus/Antispyware, filtro de dados, VPN, controle de aplicações, inspeção SSL, QoS, NAT, filtro de URL e identificação de usuários.

3.8.31 Deverão ser capaz de atualizar automaticamente as assinaturas de vírus e spyware e IPS sem a necessidade de intervenção humana.

3.8.32 Deve implementar e estar devidamente licenciada para, no mínimo, 200(duzentos) túneis de VPN IPSEC simultâneos;

3.8.33 Os dispositivos de proteção de rede devem possuir, pelo menos, as seguintes funcionalidades:

3.8.33.1 Suporte a, no mínimo, 200 (duzentos) VLAN Tags 802.1q;
3.8.33.2 Agregação de links 802.3ad e LACP;
3.8.33.3 Policy based routing ou policy based forwarding;
3.8.33.4 Roteamento multicast (PIM-SM);
3.8.33.5 DHCP Relay;
3.8.33.6 DHCP Server;

3.8.33.7 Deve permitir a criação de sub-interfaces ethernet lógicas.

3.8.34 Deve suportar os seguintes tipos de NAT:

3.8.34.1 NAT dinâmico (Many-to-1);
3.8.34.2 NAT dinâmico (Many-to-Many);
3.8.34.3 NAT estático (1-to-1);
3.8.34.4 NAT estático (Many-to-Many);
3.8.34.5 NAT estático bidirecional 1-to-1;
3.8.34.6 Tradução de porta (PAT);
3.8.34.7 NAT de Origem;
3.8.34.8 NAT de Destino;
3.8.34.9 Suportar NAT de Origem e NAT de Destino simultaneamente.

3.8.35 Deve permitir o envio de logs para sistemas de monitoramento externos.

3.8.36 Deve prover mecanismo de prevenção a ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deverá se originar ou proteções de zona para ataques de Flood e ataques de reconhecimento.

3.8.37 Deve permitir o bloqueio de sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo, desta forma, possíveis tráfegos maliciosos.

3.8.38 Deve ser possível visualizar o motivo para o término da sessão no firewall, através dos logs de tráfego ou troubleshooting, incluindo sessões finalizadas onde houver de-criptografia de SSL.

3.8.39 Deverão suportar sub-interfaces lógicas;

3.8.40 Implementar roteamento estático para o IPV4 e IPV6;

3.8.41 Deverá possuir ferramentas para depuração e gerenciamento em primeiro nível para IPv4 e IPv6, implementando, ao menos, testes ICMP, debug, trace e log de eventos;

3.8.42 Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPFv2);

3.8.43 Deve suportar, no mínimo, as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4, IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL, PBF/PBR (Policy Based Forwarding/ Policy Based Routing), DHCPv6 Relay, IPSEc, SNMP, NTP, DNS e controle de aplicação.

3.8.44 Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas, nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

3.8.44.1 *Modo Sniffer*, para inspeção via porta espelhada do tráfego de dados da rede;

3.8.44.2 *Modo Camada – 2 (L2)*, para inspeção de dados em linha, com visibilidade e controle do tráfego em nível de aplicação;

3.8.44.3 *Modo Camada – 3 (L3)*, para inspeção de dados em linha, com visibilidade e controle do tráfego em nível de aplicação, operando como default gateway das redes protegidas;

3.8.44.4 *Modo misto de trabalho Sniffer*, L2 e L3 em diferentes interfaces físicas.

Controle por Política de Firewall

3.8.45 Deve implementar controles por zona de segurança.

3.8.46 Deve implementar controles de políticas por porta e protocolo.

3.8.47 Deve implementar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

3.8.48 Deve implementar controle de políticas por usuários, grupos de usuários, endereço IP, redes e zonas de segurança.

3.8.49 Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs, podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.

3.8.50 Deve permitir criar regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários;

3.8.51 Deve possibilitar o controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).

3.8.52 Deve possibilitar o controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).

3.8.53 Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound).

3.8.54 Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 ou posterior.

3.8.55 Deve permitir bloqueios por extensão de arquivos, contemplando, no mínimo, as seguintes extensões: bat, cab, exe e possibilidade de incluir novas extensões de forma customizadas ou via regras de expressão.

3.8.56 Deve suportar QoS baseado em políticas (Prioridade, Garantia de banda e Máximo de banda).

3.8.57 Deve suportar QoS baseado em políticas para marcação de pacotes (diffserv marking).

3.8.58 Deve suportar a criação de objetos e regras IPv6.

3.8.59 Deve suportar a criação de objetos e regras multicast.

3.8.60 Suportar a filtragem de conteúdo, no mínimo, sobre os seguintes assuntos: Violência, Nudismo Pornografia, Armas, Racismo, Drogas ilegais, Crimes, Comportamento ilegal, Jogos, Álcool, Tabagismo, Conteúdo adulto, Entretenimento, Chat, Web Mail, Jogos de azar, Navegação anônima, Humor, Newsgroups, Encontros pessoais, Streaming de músicas e vídeos e Download de software (o nome da categoria pode variar de acordo com o fabricante da solução, mas o conteúdo a ser bloqueado deve ser o mesmo);

3.8.61 Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet;

3.8.62 Possibilitar a filtragem da linguagem Java script e de applets Java e Active-x em páginas WWW, para o protocolo HTTP.

3.8.63 Deve possuir antivírus de aplicação;

3.8.64 O antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3, e FTP;

3.8.65 Permitir o bloqueio de malwares (adware,spyware, hijackers, keyloggers etc.);

Controle de Aplicações

3.8.66 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

3.8.67 Deve ser possível a liberação e bloqueio somente de aplicações, sem a necessidade de liberação de portas e protocolos.

3.8.68 Deve reconhecer, pelo menos, 1500 (mil e quinhentas) aplicações diferentes, incluindo, mas não limitado a tráfego peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.

3.8.69 Deve reconhecer, pelo menos, as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, google hangouts, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote e google-docs.

3.8.70 Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta padrão ou não, por exemplo, RDP trafegando na porta 80 ao invés da porta 3389.

3.8.71 Deve identificar o uso de táticas evasivas, ou seja, possuir a capacidade de visualizar e controlar as aplicações e os ataques que utilizam tais táticas, via comunicações criptografadas, a exemplo do Skype e de ataques mediante uso da porta 443.

3.8.72 Para tráfego criptografado SSL, deve de-criptografar pacotes, a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

3.8.73 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas e validar se o tráfego corresponde com a especificação do protocolo, como aplicações encapsuladas em HTTP. A decodificação de protocolo deve, também, identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivos através do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo com as regras de segurança implementadas.

3.8.74 Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado ao WhatsApp Web.

3.8.75 Deve permitir a atualização da base de assinaturas de aplicações automaticamente, durante o período de vigência do contrato.

3.8.76 Deve reconhecer aplicações em IPv6.

3.8.77 Deve limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD.

3.8.78 Deve possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente nos controladores de domínio, nem nas estações dos usuários.

3.8.79 Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente à possibilidade de habilitar controle de aplicações em algumas regras.

3.8.80 Deve suportar múltiplos métodos de identificação e classificação das aplicações por, pelo menos, os seguintes métodos:

3.8.80.1 Checagem de assinaturas;
3.8.80.2 Decodificação de protocolos;

3.8.81 Deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

3.8.82 Deve permitir, nativamente, a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do Banco.

3.8.83 Deve alertar ao usuário quando uma aplicação web for bloqueada.

3.8.84 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.

3.8.85 Deve possibilitar a diferenciação de tráfego de aplicações Peer2Peer, possuindo granularidade de controles/políticas para os mesmos.

3.8.86 Deve possibilitar a diferenciação de tráfego de aplicações Instant Messaging, possuindo granularidade de controles/políticas para os mesmos.

3.8.87 Deve possibilitar a diferenciação e controle de ações dentro das aplicações como, por exemplo, permitir o chat e bloquear a transferência de arquivos.

3.8.88 Deve possibilitar a diferenciação de aplicações Proxies, possuindo granularidade de controles/políticas para os mesmos.

3.8.89 Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações, baseados em características das aplicações, como:

3.8.90 Nível de risco da aplicação;

3.8.91 Categoria ou sub-categoria de aplicações;

3.8.92 Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

3.8.93 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL, devidamente licenciadas:

3.8.94 Deve ser possível a criação de políticas por usuários, grupos de usuários do Active Directory, IP e segmentos de rede;

3.8.95 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

3.8.96 Deve suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

3.8.97 Deve bloquear o acesso a sites com conteúdo indevido, ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;

3.8.98 Deve possuir, no mínimo, 60 (sessenta) categorias de URLs;

3.8.99 Deve permitir a criação de categorias de URLs personalizadas;

3.8.100 Deve permitir a exclusão de URLs do bloqueio, utilizando categorias personalizadas;

3.8.101 Deve permitir a personalização das páginas de bloqueio;

3.8.102 Deve permitir a visualização, na console de gerenciamento ou nos logs, as informações do campo x-forwarded-for do cabeçalho HTTP, nos acessos a URLs.

Prevenção de Ameaças

3.8.103 Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall.

3.8.104 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).

3.8.105 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Anti-Spyware e Antivirus: permitir, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset.

3.8.106 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoramento.

3.8.107 Deve ser possível configurar nas regras exceções por IP de origem ou de destino, de forma geral, e assinatura por assinatura.

3.8.108 Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

3.8.109 Deve ser capaz de impedir ataques básicos como: SQL Injection, Cross Site Scripting, dentre outros.

3.8.110 Deve permitir o bloqueio de métodos conhecidos de exploração de vulnerabilidades.

3.8.111 Deve permitir o bloqueio de exploits conhecidos.

3.8.112 Deve possuir os seguintes mecanismos de inspeção de IPS:

3.8.113 Análise de padrões de estado de conexões;

3.8.114 Análise de decodificação de protocolo;

3.8.115 Análise para detecção de anomalias de protocolo;

3.8.116 Análise heurística;

3.8.117 IP Defragmentation;

3.8.118 Remontagem de pacotes de TCP;

3.8.119 Bloqueio de pacotes malformados.

3.8.120 Deve ser capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, dentre outros.

3.8.121 Deve detectar e bloquear a origem de portscans.

3.8.122 Deve permitir o bloqueio de ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações.

3.8.123 Deve possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.

3.8.124 Deve possuir assinaturas para bloqueio de ataques de buffer overflow.

3.8.125 Deve possibilitar a criação de assinaturas customizadas.

3.8.126 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações.

3.8.127 Deve permitir o bloqueio de malwares, pelo menos, nos seguintes protocolos: HTTP, HTTPS e SMTP.

3.8.128 Deve suportar o controle (bloqueio/liberação) de arquivos por tipo/extensão.

3.8.129 Deve permitir, identificar e bloquear a comunicação com botnets.

3.8.130 Deve suportar várias técnicas de prevenção, incluindo Drop ou tcp-rst (Cliente, Servidor e ambos).

3.8.131 Deve suportar referência cruzada com CVE para ameaças identificadas pelo módulo de proteção de ameaças (IPS), através do próprio equipamento ou do site do fabricante.

3.8.132 Deve registrar na console de monitoramento as seguintes informações sobre ameaças identificadas:

3.8.132.1 O nome da assinatura ou do ataque;
3.8.132.2 Aplicação;
3.8.132.3 Usuário;
3.8.132.4 IP de origem da comunicação;
3.8.132.5 IP de destino da comunicação;
3.8.132.6 Ação tomada pelo dispositivo.

3.1.250 Deve suportar a captura de pacotes (PCAP);

3.2.1.251 Deve identificar o país de onde partiram os eventos de ameaças.

3.8.133 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

3.8.134 Deve permitir proteção contra downloads involuntários, usando HTTP, de arquivos executáveis maliciosos.

3.8.135 Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, dentre outros).

3.8.136 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall, considerando usuários, grupos de usuários, origem, destino e zonas de segurança. Ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas configuradas por usuários, grupos de usuários, origem, destino e zonas de segurança.

Prevenção Contra Ameaças Avançadas - ATP

3.8.137 Devido aos programas maliciosos (malware), hoje em dia, serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada deve possuir funcionalidades para análise de malware não conhecido (sandbox), incluídas na própria ferramenta, ou entregue em composição com outro fabricante.

3.8.138 A solução deve prover as funcionalidades de inspeção e visibilidade de tráfego de entrada de malware não conhecido e do tipo ATP, com filtro de ameaças avançadas, e inspeção com prevenção de tráfego de saída de callbacks (comunicação do malware com o servidor de comando e controle).

3.8.139 O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise, devendo permitir a análise na nuvem do fabricante da solução, onde o arquivo será executado e simulado em ambiente controlado. Caso esta funcionalidade seja licenciada de forma separada da solução, deverão ser fornecidas todas as licenças necessárias para a utilização desta funcionalidade.

3.8.140 Deve permitir selecionar, através de políticas granulares, quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente.

3.8.141 Deve possuir a capacidade de diferenciar arquivos analisados em, pelo menos, três categorias: malicioso, não malicioso, suspeito e aguardando processamento.

3.8.142 Deve realizar a análise de arquivos maliciosos em ambiente controlado com sistema operacional Windows.

3.8.143 Deve suportar o monitoramento de arquivos trafegados na Internet (HTTPS, HTTP e SMTP), no mínimo em modo de operação Layer 3/router.

3.8.144 Deve permitir exportar o resultado das análises de malwares de dia Zero, em PDF ou CSV, a partir de uma interface de gerência.

3.8.145 Deve permitir visualizar os resultados das análises de malwares de dia zero.

3.8.146 Caso sejam necessárias licenças de sistemas operacionais e produtos de softwares para execução de arquivos no ambiente controlado, as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante.

3.8.147 Deve permitir a emulação e detecção de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir, também a análise, no mínimo, dos seguintes tipos de arquivos: Adobe Flash, Java (JAR), arquivos executáveis (EXE), PDFs, RAR e arquivos compactados (ZIP ou 7z).

3.8.148 Deve prover informações para que a solução de relatórios ou a solução de gerenciamento possa apresentar, via interface gráfica, as informações relacionadas às atividades do malware durante a execução do arquivo, nos ambientes controlados, em todas as versões de sistemas operacionais requisitados neste projeto.

3.8.149 Deve atualizar a base com a assinatura ou *hash* do arquivo infectado, para bloqueio dos malwares identificados em *sandbox* na nuvem.

Identificação de Usuários

3.8.150 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local.

3.8.151 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos, permitindo granularidade de controles/políticas baseadas em usuários e grupos de usuários do AD, sem a necessidade de instalação de agente nos controladores de domínio ou nas estações dos usuários.

3.8.152 Deve possuir integração com RADIUS, para identificação de usuários e grupos, permitindo granularidade de controles/políticas baseadas em usuários e grupos de usuários.

3.8.153 Deve possuir integração com LDAP, para identificação de usuários e grupos, permitindo granularidade de controles/políticas baseadas em usuários e grupos de usuários.

3.8.154 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída para a Internet, sendo que, antes de iniciar a navegação, deve apresentar, para o usuário, portal de autenticação residente no firewall (Captive Portal).

3.8.155 Deve identificar usuários através de leitura do campo x-forwarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso.

3.8.156 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

3.8.157 Deve possuir suporte para identificação de múltiplos usuários conectados em um mesmo endereço IP, em servidores de terminal (Terminal Server) acessados remotamente.

QoS (Qualidade de Serviço)

3.8.158 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, como Youtube, se requer que a solução, além de poder permitir ou negar esses tipos de aplicações, deve ter a capacidade de controlá-las por políticas de utilização de banda, quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

3.8.159 Deve suportar a criação de políticas de QoS por:

- 3.8.159.1 Endereço de origem;
- 3.8.159.2 Endereço de destino;
- 3.8.159.3 Por usuário e grupo do LDAP/AD;
- 3.8.159.4 Por aplicações;
- 3.8.159.5 Por porta.

3.8.160 Deve permitir a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP, SCCP e MGCP.

3.8.161 Deve suportar QoS (traffic-shapping). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (entrada e saída).

3.8.162 Deve disponibilizar estatísticas RealTime para classes de QoS.

3.8.163 Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

Filtro de Dados

3.8.164 Deve permitir a criação de filtros para arquivos ou dados pré-definidos.

3.8.165 Deve permitir que os arquivos sejam identificados por extensão.

3.8.166 Deve ser possível identificar e, ocasionalmente, prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações.

3.8.167 Deve suportar identificação de arquivos compactados e permitir a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

Geo-localização

3.8.168 Deve suportar a criação de políticas por Geo Localização, possibilitando o bloqueio do tráfego originado em determinados países.

3.8.169 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

Antenas Wireless

3.8.170 Para os Postos, poderá atender os requisitos de Access Point descritos no Equipamento TIPO-7, interna ou externamente, ao equipamento firewall;

VPN

3.8.171 Deve implementar VPN IPSec Site-to-Site e Client-To-Site.

3.8.172 A VPN IPSec deve suportar:

- 3.8.172.1 Autenticação SHA-256 ou superior;
- 3.8.172.2 Diffie-Hellman Group 14, Group 19 e Group 20;
- 3.8.172.3 Algoritmo Internet Key Exchange (IKEv1 e v2);
- 3.8.172.4 AES 256 ou superior (Advanced Encryption Standard);
- 3.8.172.5 Autenticação via certificado IKE PKI.

3.8.173 Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSec, a partir da interface gráfica da solução ou por linha de comando, facilitando o processo de throubleshooting.

3.8.174 Dever permitir a criação de políticas de controle de aplicações, IPS, Antivírus, Antipyware e QoS para tráfego dos clientes remotos conectados na VPN, seja ela Site-to-Site ou Client-to-Site.

Hardware

3.8.175 A solução ofertada deve suportar throughput NGFW mínimo de 600 Mbps (Seiscentos megabits por segundo). O throughput deve considerar todas as funcionalidades de NGFW exigidas no Edital e seus anexos, devidamente ativadas e atuantes, simultaneamente, considerando a utilização de todas as assinaturas disponíveis, incluindo, mas não se limitando a: firewall, controle de aplicação, IPS, antivírus/antispyware. Não serão aceitas medições de capacidade cuja aferição de tráfego foi baseada em condições de teste consideradas ideais.

3.8.176 A solução ofertada deve suportar throughput mínimo de 600 Mbps (Seiscentos megabits por segundo) para Filtro de URL e inspeção SSL;

3.8.177 A solução ofertada deve suportar throughput mínimo de 600 Mbps (Seiscentos megabits por segundo) para VPN;

3.8.178 Os equipamentos ofertados devem suportar, no mínimo, 680.000 (seiscentos e oitenta mil) de sessões TCP, simultaneamente.

3.8.179 Os equipamentos ofertados devem suportar, no mínimo, 32.000 (trinta e duas mil,) novas conexões ou sessões por segundo.

3.8.180 As fontes de alimentação principal deverão funcionar com tensão elétrica de 110V~220V AC, 50~60Hz, de modo automático.

3.8.181 Deverão estar equipados com 1 (uma) porta de comunicação out-of-band para gerenciamento de configuração ou isolar uma porta de comunicação do roteador através de uma VLAN, tornando a porta totalmente isolada do ambiente de acesso;

3.8.182 A solução fornecida deve ser dimensionada para suportar todas as funcionalidades listadas no Edital e seus anexos, simultaneamente, sem degradação de performance.

3.8.183 Caso os equipamentos ofertados degradem performance da rede ou das aplicações ou, ainda, apresentem processamento superior a 90%, durante o período contratado, dentro dos parâmetros exigidos no Edital e seus anexos, a CONTRATADA deverá substituí-los por equipamentos de maior capacidade, sem ônus para o Banco, em até 30 dias corridos, contados da abertura do chamado, visando o atendimento integral ao ambiente corporativo do Banco, sem degradação de performance ou sobrecarga nos equipamentos. Todas as despesas referentes a transporte, alimentação, hospedagem e demais despesas operacionais para a substituição dos equipamentos serão de responsabilidade da CONTRATADA, sem ônus para o Banco do Nordeste.

3.8.184 Para os índices de desempenho exigidos, todas as funcionalidades solicitadas devem estar habilitadas, no nível máximo de segurança, com todas as assinaturas ativadas. A comprovação da capacidade de processamento (throughput) deverá ser feita através de testes com aferição de tráfego TCP/HTTP 64K ou um misto de protocolos diversos, que se assemelhem com o tráfego real de produção. Não serão aceitas medições de capacidade cuja aferição de tráfego foi baseada em condições de teste consideradas ideais.

Requisitos de Gerenciamento

3.8.185 Deverão apresentar uma gerência centralizada, através de padrão Web, que deverá permitir a realização de todas as configurações de Segurança necessárias. Acesso ao sistema através de cliente com browser padrão (HTTPS) e permitir o uso de duplo fator de autenticação (2FA ou MFA) para acesso à console de administração da solução.

3.8.186 Deverão estar equipados com recursos que implementem funcionalidades de gerenciamento relativas ao padrão de gerenciamento SNMP (Simple Network Management Protocol), com suporte a RFC 1213 (MIB-II), suporte a SNMPv2c, Suporte ao SNMP v3 e suporte a geração de traps; Deverá ser fornecida uma comunidade (community) SNMP de leitura em todos os equipamentos fornecidos na solução.

3.8.187 Deve ser permitido o acesso de leitura a partir de solução de NOC do BANCO ou de empresa por ele indicado, incluindo possibilidade de visualização da configuração para auditorias quando necessário.

3.8.188 Deverá permitir a visualização dos usuários conectados (cabeados ou não);

3.8.189 Suportar Internet Protocol Flow Information eXport (IPFIX), Netflow v.9 ou o equivalente;

3.8.190 Implementar o envio de mensagens de Syslog para um servidor indicado pelo BANCO;

3.8.191 A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e administração;

3.8.192 Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, com no mínimo dois níveis de permissão: total e apenas leitura;

3.8.193 Permitir a conexão simultânea de vários administradores

3.8.194 Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o firewall;

3.8.195 Possuir mecanismo para realizar remotamente, pela interface gráfica, cópias de segurança (backup) e restauração, sem a necessidade de se reinicializar o sistema (no caso de realização de backups);

3.8.196 Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação;

3.8.197 Permitir a visualização e o gerenciamento em tempo real ou com atraso não superior a 15 minutos de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall, por serviços e endereços IP de origem e destino;

3.8.198 Permitir a visualização, em forma gráfica, do percentual do uso de CPU;

3.8.199 Permitir a visualização em tempo real ou com atraso não superior a 15 minutos, dos serviços com maior tráfego e os endereços IPs mais acessados;

3.8.200 Possibilitar o controle do tráfego, pelos endereços de origem e destino da comunicação;

3.8.201 Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH;

3.8.202 Possibilitar o registro da comunicação realizada através do firewall, sob demanda do administrador, das conexões abertas e das conexões recusadas pelo mesmo;

3.8.203 Possibilitar a análise dos seus registros (LOGs) por pelo menos um programa analisador de LOG disponível no mercado;

3.8.204 Na implantação de cada firewall, a CONTRATADA deverá fornecer todas as gerências e requisitos conforme previsto no Edital, **Anexo X – Requisitos de Gerenciamento dos Serviços**. O não fornecimento desses acessos implicará em sanções administrativas de acordo com o **Anexo VI - Acordo de Níveis de Serviços**, além de não ser emitido o Termo de Aceitação Definitiva (TAD);

Controle de Acesso

3.8.205 A solução (access point, controladora ou mesmo o firewall) deverá implementar controle de acesso de forma que diferencie os tipos de usuários conectados de forma a definir o perfil do usuário;

3.8.206 A solução (access point, controladora ou mesmo o firewall) deverá permitir a atribuição de cotas mensais para cada perfil de usuário;

3.8.207 A solução (access point, controladora ou mesmo o firewall) deverá permitir atribuição de perfil de acesso para cada tipo de usuário (redes sociais, streaming, downloads, etc);

3.8.208 A identidade dos visitantes deverá ser validada através de SMS que será enviada ao número celular do mesmo no momento do cadastro;

3.8.209 O pacote de SMS deverá estar incluso na solução;

3.8.210 A solução deverá permitir o bloqueio de usuários cadastrados;

3.8.211 Deve implementar mecanismo de autenticação através de portal Web (Captive Portal) que pode ser atendido por solução em Cloud para os usuários visitantes, temporários ou clientes corporativos;

3.8.212 Deve permitir a criação de um usuário especial para gerenciamento de usuários visitantes, temporários ou clientes corporativos.

Deverá ser oferecido Treinamento de Operação de toda a solução FWNG (e solução WIFI) ofertada com carga mínima de 20h, sendo esse ministrado nas dependências do CAPGV, 4h por dia e contemplando no mínimo 1 turma de até 15 pessoas presenciais e outras 10 pessoas transmitindo remotamente via Teams onde será gravado pelo Banco do Nordeste como forma de

treinamento e documentação para os profissionais internos. O treinamento deverá ser ministrado durante ou imediatamente após a implantação, a critério do Banco, pela CONTRATADA ou por empresa contratada por este;

3.9 Requisitos dos EQUIPAMENTOS ACCESS POINTS (AP's) - EQUIPAMENTO TIPO 7

Os equipamentos *Access Point*s (AP's) que serão fornecidos para os Postos terão que atender:

3.9.1 Possuir funcionamento em modo gerenciado por Controlador Wi-Fi para configuração de seus parâmetros e visualização de forma centralizada através de padrão web/HTTPS, gerenciamento das políticas de segurança, QoS e monitoramento de RF;

3.9.1.1 As funções de controladora poderão ser fornecidas internamente aos equipamentos firewall tipo 6 ou ainda controladora Wi-Fi específica;

3.9.1.2 Todo o licenciamento necessário para as funcionalidades descritas neste termo deverá acompanhar o access point;

Características Gerais

3.9.2 Deverão ser novos, isto é, sem utilização anterior (exceto se tiverem sido utilizados com o único propósito de homologação citada neste Instrumento) e não constar em listas de *end-of-support ou end-of-life* do fabricante;

3.9.3 Possuir 01 (uma) interface de rede RJ-45 Ethernet *Auto-sensing* que suporte as velocidades de 100/1000/2.5Gbps, atendendo as especificações do padrão 802.3bz **ou** uma interface Ethernet Auto-sensing com MDI e MDX que suporte as velocidades de 10/100/1000Mbps;

3.9.4 Possuir funcionamento em modo gerenciado por Controlador Wi-Fi para configuração de seus parâmetros, gerenciamento das políticas de segurança, QoS e monitoramento de RF assim como todas a licenças necessárias;

3.9.5 Para cada equipamento entregue, deve ser entregue 1 (um) cabo UTP de 2,5 metros crimpado com RJ45 de fábrica e com a devida certificação. O mesmo deverá ser de categoria 6 ou superior. Durante ativação do Access Point, o cabo deverá ter suas extremidades etiquetadas conforme padrão definido pelo Banco durante implantação

3.9.6 Deve implementar cliente DHCP, para configuração automática de rede;

3.9.7 Deve poder operar de tal forma que realize o chaveamento (switching) do tráfego local dos usuários sem que este tráfego tenha que passar através do(s) Controlador(es) Wi-Fi (se houver controladora) - operação em modo de "chaveamento de tráfego local";

3.9.8 Deve possuir certificação da Wi-Fi Alliance para 802.11a/b/g,ac , 802.11n draft 2.0, 802.11ax e 802.11ac ou superior e implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;

3.9.9 Deve implementar o padrão de segurança WPA3, comprovando esta funcionalidade através de certificação da Wi-Fi Alliance.

3.9.10 Deve implementar os padrões 802.11a/b/g/n/ac/ax Wave 2

3.9.11 Deve possuir antenas integradas ao equipamento, compatíveis com as frequências de rádio dos padrões IEEE 802.11a/n/ac com ganho de, pelo menos, 5 dBi na faixa de 5.0 GHz e IEEE 802.11/b/g/n com ganho de, pelo menos, 3 dBi na faixa de 2.4

3.9.12 Possuir pelo menos as seguintes taxas de transmissão e com fallback automático: IEEE 802.11ac: MSC0 – MCS9 para 1 e 2 Spatial Streams (6.5Mbps - 1,3Gbps) para ambientes com até 30 usuários ou 1, 2 e 3 Spatial Streams para acima disso.

3.9.13 Possuir potência máxima de transmissão de, no mínimo, 21 dBm em 2.4GHz e 22dBm em 5GHz

3.9.14 Deverá implementar operação em 4x4:4 MIMO com diversidade espacial em 2,4 GHz;

3.9.15 Deverá implementar operação em 4x4:4 MIMO com diversidade espacial em 5 GHz;

3.9.16 Deve implementar padrão Wi-Fi 6 (802.11ax) nas frequências 2.4GHz e 5GHz simultaneamente;

3.9.17 Deve permitir a configuração da técnica "beamforming" de transmissão de forma otimizar a relação de sinal ruído e a performance de transmissão de dados para determinados usuários da rede WLAN. Deve permitir esta formação de banda para cliente 802.11 a/g/n/AC;

3.9.18 Possuir estrutura metálica que permita fixação do equipamento em teto e também em parede;

3.9.19 Possuir varredura de RF nas bandas 802.11 b/g/n e 802.11 a/n/ac para identificação de pontos de acesso intrusos não autorizados (rogues) e interferências no canal habilitado no ponto de acesso;

3.9.20 Deve possuir uma trava de segurança compatível à utilizada em desktops e notebooks (Kensington security lock ou similar) e que permita a instalação de um cabo de segurança com a finalidade de evitar o furto do equipamento. O equipamento deve vir acompanhado com o cabo de segurança.

3.9.21 Deve prover 3 Gbps por AP, considerando ambas frequências;

3.9.22 Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;

3.9.23 Implementar o protocolo de enlace CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*) para acesso ao meio de transmissão;

3.9.24 Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF;

3.9.25 Possuir suporte a pelo menos 16 SSIDs e 16 VLANs;

3.9.26 Permitir habilitar e desabilitar a divulgação do SSID;

3.9.27 Possuir padrão WMM (*Wi-Fi Multimedia*) da Wi-Fi Alliance para priorização de tráfego;

3.9.28 Não deve haver licença restringindo o número de usuários por ponto de acesso. O Ponto de Acesso deve permitir, no mínimo, 300 usuários por rádio;

3.9.29 Deve possuir no mínimo 02 rádios (dual radio) operando simultaneamente em frequências distintas;

3.9.30 Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet ou serial (terminal assíncrono);

3.9.31 Possuir, no mínimo, 01 LED indicativo do estado de operação;

3.9.32 Deve implementar um mecanismo de controle de associação de banda, de forma que usuários com capacidade de comunicação em 2,4GHz e 5GHz sejam preferencialmente, e sempre que possível, alocados nos canais da banda de 5GHz do Ponto de Acesso, quando os mesmos se associem à rede WLAN;

3.9.33 Implementar balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso, para otimizar o desempenho quando grande quantidade de usuários estão associados aos pontos de acesso;

3.9.34 Deve permitir a conexão de usuários em IPv4, IPv6 ou Dual-stack;

3.9.35 O equipamento deve ser capaz de implementar 802.11e com WMM;

3.9.36 Em conjunto com o controlador wireless, os equipamentos devem realizar a monitoração real-time das frequências de Rádio Frequência (análise espectral) em busca de interferências Wi-Fi e Interferências Não-Wi-Fi e simultaneamente atender os usuários da rede Wi-Fi;

3.9.37 Deve fazer a varredura dos espectros de 2,4 GHz e 5 GHz para identificação de interferências não 802.11, analise de espectro, e evita-las automaticamente;

3.9.38 Deve ter a capacidade de mudar de canal caso seja detectada alguma das interferências listadas no item anterior no canal de operação;

3.9.39 Deve operar nos seguintes modos: “Modo Local” e “Modo Monitor”

3.9.40 Operando em “Modo Local” o ponto de acesso deve fornecer informações ao Controlador Wi-Fi ao qual está associado referentes à qualidade do espectro de RF no canal de operação atual ao mesmo tempo que processa dados 802.11 dos usuários da rede Wi-Fi. Deve fazer tanto a transmissão de dados Wi-Fi quanto a análise de espectro simultaneamente, sem prejuízo ao fornecimento de Wi-Fi aos usuários;

3.9.41 Operando em “Modo Monitor” deve fornecer informações ao Controlador Wi-Fi referente à qualidade do espectro de RF para todos os canais monitorados em 2.4GHz e em 5GHz, simultaneamente, identificando equipamentos interferentes na rede Wi-Fi e rogue APs;

3.9.42 Deverão estar equipados com recursos que implementem funcionalidades de gerenciamento relativas ao padrão de gerenciamento SNMP (*Simple Network Management Protocol*), com suporte a RFC 1213 (MIB-II), suporte a SNMPv2c, Suporte ao SNMP v3 e suporte a geração de *traps*; Deverá ser fornecida uma comunidade (community) SNMP de leitura em todos os roteadores fornecidos na solução.

Segurança da Informação

3.9.43 Implementar WPA-2 (Wi-Fi Protected Access com algoritmo de criptografia AES, 128 bits).

3.9.44 Deverá implementar WPA-3

3.9.45 Implementar segurança IEEE 802.11i;

3.9.46 Suportar a criptografia centralizada com os seguintes protocolos: AES-CCMP e TKIP ;

3.9.47 Realizar a varredura no canal de operação do AP sem impacto na performance da rede WLAN;

3.9.48 Permitir a varredura em todos os canais possíveis de RF para detecção e contenção de ameaças na rede WLAN;

3.9.49 Deve fazer a varredura dos espectros de 2,4 GHz e 5 GHz para identificação de interferências não 802.11, analise de espectro, e evita-las automaticamente;

3.9.50 Utilizar os APs como ”sensores” de RF para fazer a monitoração do ambiente Wireless;

3.9.51 Implementar mecanismos para detecção de APs não autorizados (rogues);

3.9.52 Realizar a contenção automática dos APs Rogue através da rede WLAN;

3.9.53 Realizar a identificação e contenção de redes “AD-HOC;

3.9.54 Em conjunto com o controlador wireless, deve implementar funcionalidades de WIPS (Wireless Intrusion Prevention System) com detecção de ataques à rede sem fio e tomada automática de ações de defesa no próprio conjunto de AP;

Alimentação

3.9.55 Possibilitar a alimentação via padrão PoE (802.3af ou PoE+ (IEEE 802.3at), utilizando apenas uma porta do switch onde estiver conectado;

3.9.56 Todos os Access Points deverão sem alimentados por portas PoE do próprio equipamento firewall ou switch ofertados no item do EQUIPAMENTO TIPO 6 ou através de *power injectors* fornecidos pela CONTRATADA.

Gerenciamento

3.9.57 Acesso ao sistema através de cliente com browser padrão (HTTPS);
3.9.58 Permitir monitoramento centralizado com visualização de todos os Access Points com identificação dos Postos onde estão instalados;
3.9.59 Permitir realizar varredura de RF contínua ou sob demanda, com identificação de APs irregulares;
3.9.60 Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura e controle da propagação indesejada de RF;
3.9.61 Implementar sistema de balanceamento de carga para associação de clientes entre APs próximos, para otimizar a performance;
3.9.62 Ajustar, dinamicamente, o nível de potência e canal de rádio dos APs, de modo a otimizar o tamanho da célula de RF, garantindo a performance e escalabilidade;
3.9.63 Permitir o uso de voz e dados sobre um mesmo SSID;
3.9.64 Otimizar o desempenho e a cobertura da radiofrequência;
3.9.65 Possuir base de dados de usuários interna para autenticação de usuários convidados / temporários (acesso guest)
3.9.66 Realizar o provisionamento de usuários convidados (guests) através de interface Web por meio de um usuário administrativo com permissões mínimas, exclusivas para este fim
3.9.67 Permitir o bloqueio de comunicação entre clientes wireless – L2 bridging;
3.9.68 Implementar filtros baseados em protocolos;
3.9.69 Implementar listas de controle de acesso (ACLs);
3.9.70 Permitir a aplicação de políticas de camada 4, de acordo com as características do usuário. Por exemplo, um usuário que pertença ao grupo de gerentes (cadastrado no Radius ou Active Directory) terá permissão de acesso ao protocolo FTP no servidor de ERP;
3.9.71 Implementar Qualidade de Serviço com a marcação de pacotes utilizando Diffserv e suporte a 802.1p para QoS de rede;
3.9.72 Permitir o controle de banda disponível por categoria de sites web;
3.9.73 Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoIP, VoWLAN, videoconferência, dentre outras;
3.9.74 Implementar roaming de camada 2 e de camada 3;
3.9.75 Na implantação, a CONTRATADA deverá fornecer todas as gerências e requisitos conforme previsto no Edital, **Anexo X – Requisitos de Gerenciamento dos Serviços**. O não fornecimento desses acessos implicará em sanções administrativas de acordo com o **Anexo VI - Acordo de Níveis de Serviços**, além de não ser emitido o Termo de Aceitação Definitiva (TAD);

4 MEIOS FÍSICOS DOS CIRCUITOS PRIMÁRIOS, SECUNDÁRIOS E TERCIÁRIOS (ITEM 1)

4.1 Os circuitos de acesso primários, secundários e terciários das Unidades Distribuídas, postos, Parceiros, Site Secundário (independente da localidade/tecnologia) e do Site Primário (CAPGV) deverão constituir-se de meios físicos terrestres ou 5G e dedicados, independentes, podendo cada trecho que compõe cada circuito de acesso ser constituído exclusivamente por um ou mais dos seguintes meios:

- Fibra óptica;
- Cabo metálico; ou

- 5G.

4.2 Deverá ser observado ainda que o circuito primário, secundário e terciário não compartilharão os mesmos recursos de acesso ao meio e Pontos de Presença, exceto em casos onde for fisicamente impossível;

4.3 A última milha deverá obrigatoriamente ser fornecida por meio terrestre (fibra óptica ou cabo metálico).

5 REQUISITOS ESPECÍFICOS PARA O SITE PRIMÁRIO CAPGV E SITE SECUNDÁRIO (ITEM 1)

5.1 Quantidade de equipamentos roteadores e comutadores

5.1.1 Deverão ser fornecidos equipamentos roteadores em quantidade suficiente para suportar o tráfego de/para cada um dos grupos especificados, independentemente. Esse requisito aplica-se ao conjunto de todas as unidades distribuídas, e separadamente à conexão com os parceiros do Banco, respeitando os demais requisitos aplicáveis.

5.2 Capacidade dos equipamentos roteadores e comutadores

5.2.1 Os equipamentos roteadores e comutadores fornecidos deverão ser capazes de trafegar, sem a ocorrência de subdimensionamento, toda a largura de banda disponível entre a concentração e as unidades distribuídas, incluindo a largura de Internet.

5.2.2 A título de roteamento de tráfego (throughput) os concentradores MPLS deverão suportar a soma dos links das Unidades, conforme **Anexo III - Endereços e Velocidades do Edital**, permitindo crescimento de 100% (cem por cento), sem a necessidade de troca dos equipamentos na concentração e unidades distribuídas.

5.2.3 Os equipamentos roteadores utilizados nos concentradores (Site Primário e Site Secundário) para a Internet deverão possibilitar o aumento na capacidade para processamento de tráfego IMPLEMENTADA especificada para cada roteador, permitindo crescimento de 100% (cem por cento), sem a necessidade de troca dos equipamentos na concentração.

5.3 Capacidade de instalação e remoção de módulos e interfaces

5.3.1 Deverão ser fornecidos equipamentos que permitam a adição e remoção de módulos e interfaces de rede sem a necessidade de desligamento ou reinício do mesmo (mecanismo conhecido como “Hot Swap”), de forma a permitir a troca de componentes do equipamento sem afetar a conectividade com outros circuitos que não sejam atendidos pelo componente defeituoso.

5.4 Infraestrutura de Acesso no Concentrador

5.4.1 Deverá ser provida infraestrutura de acesso totalmente redundante nos concentradores conforme abaixo detalhado:

Site Primário

5.4.1.1 **Roteador concentrador primário das Unidades Distribuídas**: 01 acesso redundante (sem compartilhamento de última milha e POP) para a rede primária MPLS (Operadora_1);

5.4.1.2 **Roteador concentrador primário Parceiro**(Operadora_1)**:** 01 acesso para a rede primária MPLS dos Parceiros;

5.4.1.3 **Roteador concentrador primário Parceiro**(Operadora_2)**:** 01 acesso para a rede primária MPLS dos Parceiros;

Site Secundário

5.4.1.4 **Roteador concentrador secundário das Unidades Distribuídas**: 01 acesso redundante (sem compartilhamento de última milha e POP) para a rede primária MPLS (Operadora_1);

5.4.1.5 **Roteador concentrador secundário Parceiro**(Operadora_1)**:** 01 acesso para a rede secundária MPLS dos Parceiros;

5.4.1.6 **Roteador concentrador secundário Parceiro**(Operadora_2)**:** 01 acesso para a rede secundária MPLS dos Parceiros;

5.4.2 Considerando que a rede Parceiros prevê o provimento remoto com duas operadoras distintas (Operadora 1 e 2, link primário e secundário), os acessos concentradores acima deverão considerar a chegada de ambas as operadoras em ambos os datacenters. Por isso, a quantidade de acessos acima informada é a mínima.

5.4.3 Para cada acesso concentrador MPLS Parceiros será fornecido pela CONTRATADA um CPE concentrador seguindo as especificações já descritas;

5.4.4 Devendo os circuitos de comunicação utilizar tecnologia determinística e ter encaminhamentos distintos para interligar-se ao ponto de presença do fornecedor. Os concentradores da Rede Parceiros não poderão ser compartilhados com os outros concentradores.

5.5 Redundância e recuperação automática de falhas

5.5.1 No caso de falha em qualquer um dos recursos de acesso no concentrador, equipamento roteador, interface ou porta de equipamento, ou qualquer outra falha em componente fornecido que afete os serviços, todo o tráfego afetado deverá ser redirecionado para os outros recursos que permaneçam em operação, devendo todas as características e funcionalidades do serviço serem mantidas plenamente, mantendo-se atendido ainda o requisito de capacidade de transmissão para cada circuito de acesso em operação. Essa comutação deverá ser realizada na nuvem da operadora contratada.

5.5.2 O restabelecimento dos serviços em caso de falha e o retorno à operação normal quando do fim da falha deverão acontecer, em sua plenitude, de forma automática em até 3 (três) minutos a partir do início ou fim da falha. Isto deve acontecer sem qualquer intervenção humana, quer seja para realizar configuração em equipamento ou sistema de gerência, quer seja para realizar mudanças físicas na infraestrutura fornecida.

5.6 Distribuição de carga nos circuitos de acesso

5.6.1 A implementação da solução do CONTRATADA **do ITEM 1** . deverá assegurar a divisão do tráfego através da funcionalidade de distribuição de carga entre os enlaces de acesso primário e secundário, de forma totalmente transparente para o Banco. Esse critério deverá ser aplicado independentemente, tanto para a capacidade de transmissão quanto de recepção.

5.6.2 Deverá ser possível também a implementação da distribuição da carga entre os roteadores concentradores localizados no Site Primário e Site Secundário.

6 REQUISITOS ESPECÍFICOS PARA OS CIRCUITOS DE ACESSO REMOTOS

6.1 Requisitos específicos para os Circuitos de Acesso Primário (MPLS) (Unidades Distribuídas e Parceiros)

Cada unidade distribuída e Parceiro deverá ser atendida por um circuito de acesso primário, que utilizará tecnologia determinística para conexão ao backbone MPLS e dará o suporte ao tráfego de dados, voz e imagens (quando houver) da respectiva unidade distribuída.

As tecnologias secundárias e terciárias deverão possuir meios físicos completamente diferentes e independentes entre si e dos sistemas fornecidos para os circuitos de acesso primários, isto é, sem que haja compartilhamento de recurso entre os circuitos de acessos primário, secundário e terciário, incluindo subsestações e pontos de presença.

Caso não haja meios distintos de acesso de entrada na Unidade Distribuída (ex: postes e dutos subterrâneos), os acessos primários, secundários e terciários poderão compartilhar o acesso que já estiver previamente instalado.

6.1.1 Instalação do circuito

Todos os serviços necessários à instalação do circuito, tais como passagem de cabos e tubulações, ficarão a cargo da CONTRATADA.

6.1.2 Capacidade dos circuitos de acesso

A capacidade de transmissão mínima dos circuitos de acesso das unidades distribuídas está especificada no **Anexo III - Endereços e Velocidades**. Tal capacidade já considera o tráfego integrado de dados, voz e imagens a ser gerado de/para cada unidade distribuída, conforme indicado no próprio Anexo.

A capacidade de transmissão especificada deverá ser do tipo full duplex, ou seja, a mesma capacidade para transmissão e recepção deverá estar disponível simultaneamente.

6.2 Requisitos específicos para os Circuitos de Acesso Secundários (MPLS - Parceiros e Internet Determinística - Unidades Distribuídas)

Todos os Parceiros serão atendidos por circuito de acesso secundário do tipo MPLS, conforme item anterior.

Entretanto, as unidades distribuídas serão atendidas por um circuito de acesso secundário do tipo Internet Determinística Simétrica, isto é, dedicada e com garantia de 100% (cem por cento) do tráfego de upload e download. Este acesso deverá ser determinístico e utilizará os meios abaixo que darão suporte ao tráfego de dados, voz e imagens (quando houver) da respectiva unidade distribuída.

Essas tecnologias deverão possuir meios físicos completamente diferentes e independentes dos sistemas fornecidos para os circuitos de acesso primários, isto é, sem que haja compartilhamento de qualquer tipo de recurso entre o circuito de acesso primário e o circuito de acesso secundário.

Cada circuito de acesso secundário de Internet Determinística deverá ser fornecido juntamente com o 01 (um) endereço IP público, exclusivo e dedicado àquela unidade distribuídas, assim como a sua respectiva máscara e default gateway.

Todas as tecnologias acima estarão sujeitas aos requisitos de SLA estabelecidos no **Anexo VI - Acordo de Níveis de Serviços** e poderão, a critério do Banco e respeitando a cobertura da CONTRATADA, serem alteradas durante a vigência contratual.

6.2.1 Instalação do circuito

Todos os serviços necessários para instalação do circuito, tais como passagem de cabos e tubulações ficarão a cargo da CONTRATADA.

6.2.2 Capacidade dos circuitos de acesso

A capacidade de transmissão mínima dos circuitos de acesso das unidades distribuídas está especificada no **Anexo VIII - Endereços e Velocidades**. Tal capacidade já considera o tráfego integrado de dados, voz e imagens (quando houver) a ser gerado de/para cada unidade distribuída, conforme indicado no próprio Anexo.

A capacidade de transmissão especificada deverá ser do tipo full duplex, ou seja, a mesma capacidade para transmissão e recepção deverá estar disponível simultaneamente, de forma dedicada, isto é, 100% (cem por cento) para download e 100%(cem por cento) para upload.

6.3 Requisitos específicos para os Circuitos de Acesso Terciários (Internet Simétrica ou Assimétrica) (Unidades Distribuídas)

Cada Unidade Distribuída deverá ser atendida por um circuito de acesso terciário do tipo Internet Simétrica ou Assimétrica, de acordo com a disponibilidade da CONTRATADA. Este acesso utilizará os meios físicos já especificados.

Cada circuito de acesso terciário Simétrico deverá ser fornecido juntamente com o 01 (um) endereço IP público, exclusivo e dedicado àquela Unidade, assim como a sua respectiva máscara e default gateway.

Caso durante a vigência contratual a CONTRATADA do **ITEM 1** apresente disponibilidade de atendimento em tecnologia superior a porventura instalada (mantendo os aspectos de independência dos demais acessos), por exemplo: MPLS para Internet ou Internet Simétrica em detrimento da Internet Assimétrica, este se obriga a informar a viabilidade ao Banco e a enviar proposta de preço para realização de aditivo, a critério do Banco, para alteração da tecnologia.

Todas as tecnologias acima estarão sujeitas aos requisitos de SLA estabelecidos no **Anexo XI - Acordo de Níveis de Serviços** e poderão, a critério do Banco, e respeitando a cobertura da CONTRATADA, serem alteradas durante a vigência contratual.

6.3.1 Instalação do circuito terciário

Todos os serviços necessários para instalação do circuito, tais como passagem de cabos e tubulações ficarão a cargo da CONTRATADA.

6.3.2 Capacidade dos circuitos de acesso

A capacidade de transmissão mínima dos circuitos de acesso das unidades distribuídas está especificada no **Anexo III - Endereços e Velocidades**. Tal capacidade já considera o tráfego integrado de dados, voz e imagens (quando houver) a ser gerado de/para cada unidade distribuída, conforme indicado no próprio Anexo.

A capacidade de transmissão especificada para os acessos simétricos determinísticos deverá ser do tipo full duplex, ou seja, a mesma capacidade para transmissão e recepção deverá estar disponível simultaneamente, de forma dedicada, isto é, 100% (cem por cento) para download e 100%(cem por cento) para upload.

Caso seja fornecido acesso assimétrico, durante a vigência contratual, a capacidade de transmissão e recepção deverá atender os limites estabelecidos pela ANATEL pela Resolução Resolução nº 717/2019. Atualmente, a ANATEL estabelece que a largura de banda média percebida ao final do mês não pode ser inferior a 80% (oitenta por cento) para download e upload. Estando sujeito a alterações, conforme regulamentações da ANATEL.

6.4 Requisitos específicos para os Circuitos de Acessos Primários e Secundários (Internet Simétrica e Simétrica/Assimétrica) (Postos)

Todos os Postos serão atendidos por um dos circuitos de acesso tipo Internet Determinística, isto é, dedicada e com garantia de 100% (cem por cento) do tráfego de upload e download. Estes acessos deverão ser determinísticos e utilizarão os meios físicos abaixo que darão suporte ao tráfego de dados, voz e imagens (quando houver) da respectiva unidade distribuída.

O segundo circuito de acesso Internet poderá ser do tipo Assimétrico (na ausência de viabilidade de Internet Simétrica). Caso, durante a vigência contratual do **ITEM 1** , apresente disponibilidade de atendimento com tecnologia superior a porventura instalada (mantendo-se os aspectos de independência dos demais acesso), a CONTRATADA se obriga a informar a viabilidade ao BANCO, para uma possível troca, a critério do Banco.

Cada circuito de acesso Internet Determinística deverá ser fornecido juntamente com o 01 (um) endereço IP público, exclusivo e dedicado àquela unidade distribuídas, assim como a sua respectiva máscara e default gateway.

Todas as tecnologias acima estarão sujeitas aos requisitos de SLA estabelecidos no Anexo VI - Acordo de Níveis de Serviços e poderão, a critério do Banco e respeitando a cobertura da CONTRATADA, serem alteradas durante a vigência contratual.

Os acessos deverão possuir meios físicos completamente diferentes e independentes entre si;

6.4.1 Instalação do circuito

Todos os serviços necessários para instalação do circuito, tais como passagem de cabos e tubulações ficarão a cargo da CONTRATADA.

Será de responsabilidade da CONTRATADA a instalação física inicial de todos os equipamentos, incluindo Access Points e demais equipamentos para atender os itens deste edital, sem ônus adicional para o BANCO;

6.4.2 Capacidade dos circuitos de acesso

A capacidade de transmissão mínima dos circuitos de acesso dos postos está especificada no **Anexo III - Endereços e Velocidades**. Tal capacidade já considera o tráfego integrado de dados, voz e imagens (quando houver) a ser gerado de/para cada Unidade Distribuída, conforme indicado no próprio Anexo.

A capacidade de transmissão especificada deverá ser do tipo full duplex, ou seja, a mesma capacidade para transmissão e recepção deverá estar disponível simultaneamente, de forma dedicada, isto é, 100% (cem por cento) para download e 100%(cem por cento) para upload.

6.5 Chaveamento entre os circuitos de acesso pela solução SD-WAN (ITEM 2)

Ao longo do Contrato, deverá ser possível ao Banco a qualquer momento, de acordo com endereço IP e porta de suas aplicações, definir critérios de chaveamento entre os circuitos de acesso da Unidade. Este chaveamento deverá ser automático ou manual, a critério do Banco.

No chaveamento automático, deverá ser possível definir para cada aplicação do Banco (IP/porta) qual circuito de acesso utilizar, baseado em critérios de disponibilidade e performance/qualidade dos circuitos de acesso disponíveis no momento, conforme requisitos desta especificação.

6.6 Chaveamento para o Site Secundário (ambos os ITENS)

Em caso de queda do Site Primário (CAPGV), todo o tráfego oriundo das unidades distribuídas, Parceiros e Postos deverá ser chaveado (roteado) para o Site Secundário. A critério do Banco, tal chaveamento poderá ser manual, isto é, com intervenção humana e agendado com o Banco, ou automático, isto é, sem intervenção humana. O método inicial será informado no momento da implantação aos CONTRATADAS.

Também a critério do Banco, o tráfego de determinada operadora poderá ser direcionado para o Site Primário (CAPGV) e/ou Site Secundário.

6.7 Plano de Upgrade para a Solução em Ambiente em Produção

Com base na expectativa de aumento na quantidade de Unidades Distribuídas e/ou Postos, assim como possível incremento de banda dos circuitos atualmente identificados no **ANEXO III – Endereços e velocidades**, o Banco reservará um percentual de **até 5%** (cinco por cento) do valor do contrato atual para atender a estas demandas, durante a vigência do contrato.

Prevalecem os requisitos de crescimento e aumento de banda de todos os equipamentos, conforme já descrito no Edital, os quantitativos informados na Tabela de Serviços sob Demanda representam apenas uma reserva para serviços que não precisarão de aditivação no contrato atual.

Identificada a necessidade, por parte do Banco, será enviado e-mail à CONTRATADA, com solicitação de upgrade de um link atual (para um perfil de banda disponibilizado neste contrato) ou solicitação de adição de nova unidade, para que a CONTRATADA possa atender a solicitação, sem a necessidade de aditivo contratual, considerando os prazos previstos no **ANEXO XI - ACORDO DE NÍVEIS DE SERVIÇO**.

Os Serviços sob demanda representam uma contingência para o caso de ampliação de banda de Unidades Distribuídas atuais ou criação de novas Unidades Distribuídas/Postos. Os quantitativos não representam obrigação de Contratação por parte do Banco, apenas para utilização caso haja crescimento de demanda/necessidade e sua solicitação ficará a critério do Banco sem necessidade de aditivo no contrato para solicitação dos serviços. Para ambos os casos a OPERADORA será consultada sobre a viabilidade.

Após o atendimento da solicitação, será gerado um **Termo de Ampliação do Remoto (TAR)** e, no mês subsequente, deverá ser enviada planilha com as quantidades de sites e Banda para batimento dos valores a serem pagos, conforme modelo de Proposta, (**Anexo II – Modelo de Proposta**, respeitando os valores já firmados para unidades com a mesma velocidade no mesmo estado da federação.

7 APLICAÇÃO DE POLÍTICAS DE CONTROLE DE TRÁFEGO

7.1 Os serviços deverão ser prestados de modo a possibilitar o controle do tráfego de dados, voz e imagens, de acordo com as classes de serviços definidas neste Anexo. O controle do tráfego deverá ser baseado, dentre outros, nos seguintes parâmetros:

7.1.1 Endereços de origem e destino do Internet Protocol (IP);

7.1.2 Portas de origem e de destino relacionadas aos diversos protocolos que operam em conjunto com o Internet Protocol (IP).

7.1.3 No tráfego previamente marcado pela solução de SD-WAN e/ou marcado pelos equipamentos do Banco.

7.1.4 No caso da tecnologia MPLS, a rede do CONTRATADA deverá suportar todas as funcionalidades de VPN, MPLS e QoS. Deverão ser seguidos os seguintes padrões das RFCs 2474 e 2475 – DiffServ, complementados pela RFC 2597 – Assured Forwarding Per-hop Behaviors (AF PHB) e pela RFC 2598 – Expedited Forwarding (EF).

7.1.5 Os valores de largura de banda que são definidos no Anexo III - Endereços e Velocidades para cada classe de serviço (imagem, voz e dados de alta, média e baixa prioridade) representam os limites mínimos garantidos da utilização de cada classe. Caso uma determinada classe não esteja utilizando a capacidade total da largura de banda alocada para a mesma, essa capacidade excedente poderá ser utilizada por outras classes de serviço, respeitando a priorização de tráfego definida pelo Banco no item 4 deste anexo. Exceto as classes de voz e imagem, que não poderão extrapolar o limite estabelecido.

7.1.6 No caso dos links MPLS, deverá ser possível realizar o transbordo de uma classe para outra classe, realizando a remarcação do pacote. Por exemplo, no caso de uma classe que marque um pacote AF31 chegar a seu limite de ocupação de largura de banda, deverá ser possível encaminhar o tráfego como transbordo, remarcando esse para AF12, por exemplo, onde esse respeitará as regras definidas na nova classe. O critério será informado pelo Banco em fase de implantação, podendo ser alterado durante o Contrato.

7.1.7 Ainda sobre os links MPLS, deverá ser possível manter a marcação DSCP realizada na LAN por outros equipamentos e realizar a devida priorização, ou seja, o algoritmo de classificação deverá permitir a priorização com base no DSCP, mesmo quando pacotes internos da LAN tiverem o mesmo IP de origem e marcações DSCP diferentes. A solução SD-WAN do Banco realizará tuneis entre os sites, inclusive para links MPLS. Por esse motivo, o mesmo IP de origem da interface do dispositivo SD-WAN será usado para diferentes origens e priorizações internas. Além de utilizar a marcação DSCP recebida da LAN, os roteadores das operadoras poderão, a critério do Banco, possuir também uma lista (ACL) definida com IP e porta dos principais serviços do Banco.

7.1.8 As configurações referentes à probabilidade de descarte de pacotes, especificadas na RFC 2597, deverão ser suportadas pela Rede MPLS, porém não serão utilizadas num primeiro momento, podendo, no futuro, serem solicitadas para que seja possível a escolha de tráfegos específicos que terão pacotes descartados antes dos outros.

7.1.9 A CONTRATADA do ITEM 1 deverá prover uma rede IP logicamente independente e isolada de qualquer outra rede, em especial do ambiente público da Internet. O mecanismo para implementar o isolamento e a qualidade de serviços é o MPLS/VPN. Essa garantia deverá ser implementada “fim-a-fim”.

Fornecimento de informações

Quando da implantação dos serviços, caberá ao Banco o fornecimento de todas as informações sobre sua infraestrutura de tecnologia, desde que pertinentes aos serviços ora especificados, de modo a permitir a adequada configuração dos componentes envolvidos nos serviços, incluindo:

- Plano de endereçamento utilizado pelo Internet Protocol (IP) na rede interna do Banco e unidades remotas;
- Protocolos de roteamento utilizados;
- Detalhamento de regras e políticas de controle e qualificação de tráfego;

- Detalhamento da caracterização do tráfego de dados, voz e imagens, incluindo suas possíveis subclassificações;
- Padrão de configuração de sistema operacional de roteadores e comutadores.

8 REQUISITOS GERAIS PARA OS EQUIPAMENTOS APPLIANCES SD-WAN (ITEM 2)

Todos os equipamentos *appliances* a serem fornecidos para atender os serviços de SD-WAN nas Unidades Distribuídas do Banco, no Site Primário e Site Secundário deverão atender ao seguinte conjunto de requisitos:

8.1 Os equipamentos *appliances* SD-WAN destinam-se para uso nas Unidades Distribuídas e Datacenters. Não está previsto o seu uso na Rede Parceiros e Postos neste primeiro momento. Havendo necessidade, a critério do Banco, aditivos contratuais de expansão serão providenciados;

8.2 A solução será composta pelos serviços do SASE NOC (Network Operations Center).

8.3 Deverão ser novos, isto é, sem utilização anterior (exceto se tiverem sido utilizados com o único propósito de homologação citada neste edital);

8.4 Todos os produtos que compõem a solução devem ser fornecidos com o devido licenciamento, incluindo garantia de atualização de software, de manutenção e de troca do hardware pelo período de vigência do Contrato estabelecido pelo Edital;

8.5 Todas as funcionalidades devem estar disponíveis na versão atual da solução ofertada, não serão aceitos equipamentos cujas funcionalidades ainda estão em desenvolvimento (Roadmap);

8.6 Deverão possuir LED's indicativos do estado de funcionamento do equipamento;

8.7 Os equipamentos fornecidos para SD-WAN nas Unidades Distribuídas deverão implementar "zero-touch" em sua primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração do equipamento via sistema de gerenciamento SD-WAN, mesmo antes do equipamento ser conectado à rede, transformando a atividade remota em uma simples troca física de equipamento, em caso de falha do mesmo, sem a necessidade de configurações individuais nos equipamentos. O Banco entende por zero-touch a possibilidade de conexão do equipamento na unidade remota e somente com um link de internet ativo o equipamento deverá consultar a nuvem do fabricante e entender que deve ser gerenciado pela solução instalada no Banco (on-permise) ou em nuvem e receber toda a configuração de forma automática sem a necessidade de nenhum tipo de configuração posterior no equipamento remoto, mesmo antes da instalação física;

8.8 A solução SD-WAN deverá ocupar no máximo 2Us (Rack units) em cada Unidade Distribuída e receberá as conexões dos equipamentos do Banco, sendo essas conexões de responsabilidade da CONTRATADA e entre a solução ofertada e o(s) switch(es) do Banco. Trata-se de uma conexão puramente camada 2. Deverá possuir estrutura apropriada para acondicionamento em armário de fiação (rack) de 19 polegadas ou fornecer prateleira de rack para qualquer equipamento fora desse padrão;

8.9 Nas Unidades Distribuídas, a solução de SD-WAN deverá ter capacidade para receber os acessos primários, secundários e terciários em portas do tipo **WAN**, 1Gbps, padrão Ethernet RJ-45, dedicadas para este fim;

8.10 Deverão atender aos padrões: IEEE 802.2; IEEE 802.3 e IEEE 802.3u, IEEE 802.3z;

8.11 Todas as portas utilizadas na solução deverão ser compatíveis com conexão com switches e roteadores sem necessidade de cabos cross over;

8.12 Nas Unidades Distribuídas, a solução SD-WAN deve possuir pelo menos **03 (três)** interfaces 10/100/1000Mbps, interfaces RJ-45, para cabos UTP categoria 6 enhanced

ou superior, full duplex, GigaEthernet, auto-sense, de acordo com os protocolos padrões Ethernet IEEE 802.3 10BaseT, Ethernet IEEE802.3u 100BaseTX, Ethernet IEEE802.3ab 1000BaseT e IEEE802.3z 1000BASE-X, exclusivas para conexão com a **LAN** do Banco;

8.13 A solução entregue no datacenter deve ser compatível com conexão via SFP+ utilizando fibra padrão OM4 que deverá ser entregue pela CONTRATADA, com padrão de velocidade 10Gbps e conector tipo LC no tamanho de 4 metros ou superior, de forma redundante e sem oversubscription. Toda a conectividade e redundância entre os equipamentos da solução contratada no datacenter é de responsabilidade da CONTRATADA. Devem ser fornecidas no mínimo **04 (quatro)** exclusivas para conexão com a **LAN** do Banco além de **03 (três)** interfaces para recepção dos túneis **WAN** via comunicação MPLS e Internet; O(s) transceiver(s) SFP+ necessário(s) para conexão da interface do equipamento do ITEM 2 deverão ser fornecidos em conjunto com a solução. Não será necessário o fornecimento do transceiver para conexão com a rede do Banco;

8.14 Os quantitativos de interfaces aqui especificados são mínimos. O quantitativo real necessário deverá ser considerado de acordo com o dimensionamento efetuado pela CONTRATADA, de acordo com a arquitetura ofertada;

8.15 Para cada equipamento entregue, deve ser entregue 03 (três) cabos UTP de 2,5 metros crimpados com RJ45 de fábrica e com a devida certificação. Os mesmo deverão ser de categoria 6 ou superior. Durante ativação do roteador, o cabo deverá ter suas extremidades etiquetadas conforme padrão definido pelo Banco durante implantação;

8.16 Nos Datacenters, em caso de fornecimento de solução SD-WAN com mais interfaces de conexão, compatíveis com as velocidades 1/10/40Gbps, todas devem ser licenciadas para uso a critério do Banco e devem ser entregues com transceivers de fibra instalados e licenciados. Para os casos com mais de 2 interfaces 10/40Gbps, pelo menos 02 (duas) deverão vir com transceivers de 40G, as demais poderão vir com transceivers de 1Gpbs/10Gbps. Para todas as interfaces/transceivers de fibra, deverão ser entregues fibras LC compatíveis e com tamanho de 20m mínimo;

8.17 Deverão suportar conexões no ambiente do Banco com tensão elétrica de 110V~220V AC, 50~60Hz, e deverão suportar modo automático;

8.18 Os appliances SD-WAN ofertados destinados aos Datacenters devem possuir fontes redundantes internas e hot-swap;

- 8.18.1 O conjunto de fontes deve possuir, pelo menos, 2 (duas) conexões independentes, permitindo a sua ligação a circuitos elétricos externos distintos;
- 8.18.2 Realizar a comutação entre as fontes de forma automática e sem qualquer interrupção no funcionamento do equipamento.
- 8.18.3 Possuir capacidade para manter a operação do equipamento em condição de consumo máximo mesmo na falha de uma fonte;
- 8.18.4 Deve ser possível visualizar o status das fontes ou gerar alarme no caso de falha em qualquer delas. O alarme deve aparecer em console central;

8.19 A solução SD-WAN deve obedecer ao princípio básico da arquitetura SDN (Software Defined Networks) separando os planos de encaminhamento de tráfego, controle e gerência. Em caso de falha dos planos de controle e gerência não deve haver impacto nos serviços do plano de encaminhamento. O appliance SD-WAN deve atuar de forma eficiente no encaminhamento de tráfego, de acordo com as sinalizações vindas do elemento central de controle.

8.20 Os planos de encaminhamento (forwarding plane) e controle (control plane) devem ser logicamente independentes.

8.21 A solução deve possuir a capacidade de realizar agregação de banda para fluxo único de forma automática entre links de distintas velocidades levando em consideração a utilização de banda completa de cada link sem ocasionar congestionamento nos links de baixa velocidade.

8.22 Deverá permitir uma camada de roteamento virtual sobre a estrutura de rede tradicional, possibilitando o encaminhamento do tráfego por diferentes tipos de circuitos WAN, inclusive circuitos WAN com NAT e endereçamento dinâmico;

8.23 A solução SD-WAN deverá oferecer suporte à orquestração de túneis criptografados desde a Unidade Distribuída até o Data Center, denominados comunicação overlay, o que permitirá independência do tipo de link utilizado (comunicação underlay);

8.24 A solução deverá utilizar estes Overlays para o transporte das aplicações conforme as regras de negócio definidas, estes devem utilizar os protocolos de túnel IPSEC e GRE.

8.25 A solução SD-WAN Central deverá permitir a criação de túneis entre localidades de forma manual, automática e/ou de acordo com a intenção do tráfego.

8.26 A solução SD-WAN Central deverá possuir capacidade suficiente para suportar todas as VPN's (ou equivalentes) de todos os *appliances* das unidades remotas, assim como a quantidade prevista de ampliação, conforme **Anexo II – Modelo de Proposta**;

8.27 Caso haja necessidade de utilizar mais de 02 (dois) equipamentos para composição de throughput da solução SD-WAN central, todos os equipamentos deverão ser da mesma família e modelo, ambos licenciados para operar em modo ATIVO-ATIVO;

- 8.27.1 Caso haja necessidade de utilizar mais de 02 (dois) equipamentos SD-WAN na solução de SD-WAN central, a CONTRTATADA deverá fornecer comutadores gerenciados e redundantes para interconexão destes equipamentos a menos que utilizem portas especificas/proprietárias para interconexão da solução ou formação de cluster;
- 8.27.2 Caso sejam fornecidos equipamentos comutadores, não deve haver prejuízo para a solução ofertada no que se refere aos padrões de conectividade, redundância e nível de serviço previstos nesta especificação.
- 8.27.3 A solução deverá funcionar de forma transparente, sobretudo em relação a balanceamento das conexões e cuidados com assimetria de tráfego.

8.28 A solução SD-WAN Central deverá entregar uma gerência/orquestração integrada e resiliente para toda as unidades, não devendo criar segregação ou grupos estáticos das Unidades Distribuídas na comunicação destas com os DataCenters;

8.29 A solução deve implementar automação na formação de tuneis, por meio de associação de perfis de configuração utilizando uma única interface gráfica.

8.30 A solução deverá possibilitar que uma mesma interface WAN possa enviar tráfego simultaneamente através de túneis IPSec SD-WAN e nativamente por fora dos túneis via comunicação underlay.

8.31 A solução de SD-WAN deverá permitir criar VPNs "Full-Mesh", de forma a permitir a comunicação ponto-a-ponto dentro das redes MPLS do acesso primário, das redes MPLS do acesso secundário e dos acessos Internet Simétrica, sem passar necessariamente pelos concentradores (a critério do Banco);

8.32 A solução WAN proposta deve suportar simultaneamente hub e spoke, malha, malha parcial e topologia de malha regional na construção dos Overlays.

8.33 A solução deverá permitir ao administrador definir políticas de encaminhamento de tráfego que levem em consideração a disponibilidade dos links e as métricas de jitter, latência e perda de pacotes para selecionar, de forma totalmente automática ou manual, a critério do Banco, qual caminho uma aplicação irá utilizar de forma dinâmica.

8.34 A comutação de tráfego por pacote deve permitir que um fluxo possa mudar de um link para outro, várias vezes, sem desconectar a sessão tcp ou udp da aplicação. Em caso de falha do link essa comutação deve ocorrer em menos de 1 segundo.

8.35 A solução deve ser composta com uma Console Central de Orquestração, podendo esta ser instalada no Datacenter (on-premises) ou em nuvem do Fabricante, com conexão via Internet. A solução será responsável por fazer toda a configuração dos appliances SD-WAN, incluindo priorização de tráfego, configurações de QoS, que deverão ocorrer de forma centralizada. A console de gerenciamento SD-WAN deverá ser do mesmo fabricante dos appliances SD-WAN;

8.36 No caso da instalação da solução de gerenciamento e orquestração instalada fora no Datacenter, apenas metadados e dados de gerenciamento poderão ser transmitidos para nuvem e a solução deverá implementar duplo fator de autenticação (MFA) integrado à console em nuvem do fabricante para acesso ao portal de gerenciamento. A indisponibilidade da interface gerência e orquestração não deverá comprometer o funcionamento do serviço/configurações de SD-WAN;

8.37 Deve implementar configuração Zero Touch, onde um equipamento é ligado na localidade e via internet ele busca a configuração na Plataforma de Gerenciamento. A plataforma em Cloud deve ser Multi-Tenancy e suportar múltiplos clientes sendo gerenciados, onda cada cliente deverá possuir o seu login e ter acesso somente aos seus equipamentos.

8.38 Via gerenciamento fornecido, deverá ser possível informar quais são os links disponíveis em cada localidade, bem como a largura de banda consumida por unidade e por link;

8.39 A solução de gerenciamento e configuração dos dispositivos deve ser do mesmo fabricante de SD-WAN;

8.40 A solução de Gerenciamento deverá ser centralizada para o serviço de SD-WAN, concentrando todas as configurações via central de gerenciamento SD-WAN para todos os equipamentos envolvidos nessa solução;

8.41 Deverão permitir upgrade de sistema operacional de forma centralizada, via ferramenta de gerência, e para toda a solução, desde a cópia das novas imagens de sistema se for o caso, como a atualização em questão;

8.42 A solução deverá permitir atualização e sincronização automática de "clock", de forma que os relatórios e todas as informações sejam sincronizados com o horário oficial via NTP (Network Time Protocol);

8.43 Além da configuração centralizada, o equipamento deverá possuir forma de configuração ou acesso local via console out-of-band ou via protocolo HTTPS, sendo conexão serial ou UTP ou USB ou equivalente;

8.44 Deverão estar equipados com recursos que implementem funcionalidades de gerenciamento relativas ao padrão de gerenciamento SNMP (Simple Network Management Protocol), com suporte a RFC 1213 (MIB-II), suporte a SNMPv2c, Suporte ao SNMP v3 e suporte a geração de traps;

8.45 Permitir o gerenciamento dos tuneis VPN através de SNMP;

8.46 Deverão Implementar Network Address Translation (NAT);

8.47 Efetuar o registro em log de todos os acessos efetuados, incluindo data, hora, site, endereço IP e usuário que efetuou o acesso.

8.48 Permitir integração com servidores de log externo (syslog);

8.49 A Solução deverá permitir ao administrador criar cada localidade informando o endereço físico dessa localidade, para que a solução de gerência possa exibi-la no mapa do Dashboard em aplicativo de monitoramento entregue;

8.50 Cada solução de gerenciamento que for instalada nos datacenters (Site Principal e Site Secundário) deverá possuir redundância entre os datacenters. Isto é, caso sejam providos N-equipamentos para atender a solução de gerenciamento no Site Principal, deverão ser providos N-equipamentos para atender a solução de gerenciamento no Site Secundário, com chaveamento automático em até 3 (três) minutos sem perda de informações de gerência durante este período. Enquanto a solução estiver funcionando em contingência (com indisponibilidades no Site Principal ou Site Secundário), haverá apuração de SLA de disponibilidade;

8.51 Em nenhuma hipótese, os equipamentos da solução deverão perder a gerência por motivo de tráfego externo ou interno na unidade remota e no CAPGV. Para isso, a solução poderá implementar, caso precise, gerência out-of-band e/ou interfaces com inteligência para tratar esse tráfego, de forma que a gerência e a rede da unidade remota não fiquem indisponíveis por falha de qualquer das soluções contratadas no Edital;

8.52 Deverá implementar na própria solução todos os protocolos necessários para desempenhar o papel de SD-WAN e Gerenciamento, como por exemplo: WCCP, PBR, BGP, etc. No Site Principal e no Site secundário, a vizinhança entre o Banco e a solução SD-WAN será via roteamento estático e/ou BGP, a ser definido pelo Banco na implementação. Ainda nas redes de datacenter, a conexão lógica com os roteadores concentradores das operadoras MPLS será de responsabilidade da solução contratada, sendo puramente via BGP, se assim definido pelo Banco na implementação;

8.53 O sistema de gerenciamento deverá informar a largura de banda de Inbound e Outbound de cada circuito de comunicação, seja via cadastro manual ou de forma automática. A informação de utilização dos links deverá ser correlacionada com o tamanho real do circuito de comunicação;

8.54 A solução deverá ser capaz de fornecer via portal https visibilidade de dados trafegados por cada link em tempo real (para troubleshoot) e também via portal de relatórios (gerenciamento) após no máximo 5 minutos do tráfego em questão. A necessidade é para todos os links envolvidos e conectados nos equipamentos SD-WAN, inclusive para a comunicação entre Unidades Distribuídas, ou seja, onde o tráfego não passe pelo Datacenter;

8.55 Deverá possuir mecanismos de authentication, authorization and accounting (AAA) através de Servidor RADIUS e/ou TACACS+ e/ou Azure Active Directory e/ou outros Identity Providers;

8.56 A empresa contratada deverá fornecer dois níveis de acesso ao Banco, sendo um deles somente leitura e outro com perfil administrativo para realização de configurações, quando solicitado. Ambos os acessos devem ser fornecidos para todos os equipamentos e softwares envolvidos na solução. Os acessos de leitura deverão permitir a visualização das estatísticas do equipamento passíveis de consulta, como QoS, estatísticas de tráfego, além da configuração dos equipamentos, e qualquer política criada na solução contratada. O acesso mínimo (de leitura) deverá ser fornecido acesso via HTTPS. O acesso deverá permanecer ativo durante todo o Contrato. A solução deverá implementar auditoria sobre as alterações de configuração realizadas por cada usuário. Qualquer alteração feita pelo Banco será de responsabilidade do Banco, cabendo ao CONTRATADO, monitorar e questionar sobre a configuração realizada em até 72h corridas, tornando-se o CONTRATADO responsável pela alteração na sequência para termos de SLA de disponibilidade e demais obrigações contratuais;

8.57 No caso de um equipamento ser compatível com acesso via SSH, será obrigatório o fornecimento do acesso ao Banco, conforme detalhado acima. Utilização de acesso de telnet (sem criptografia) para gerenciamento não será permitido no Banco;

8.58 Deverá ser fornecido usuário de leitura para o Banco para todos os equipamentos e softwares que compõem o ITEM 2;

8.59 O não fornecimento de quaisquer desses acessos implicará em sanções administrativas de acordo com o Anexo VI - Acordo de Níveis de Serviços, além de não ser emitido o Termo de Aceitação Definitiva (TAD);

8.60 Necessariamente, a solução de SD-WAN contratada nas remotas será o default gateway dos equipamentos naquela unidade remota (estações de trabalho, aparelhos IP, servidores, impressoras, etc.);

8.61 A solução deverá fornecer IP via DHCP server, sendo fornecimento próprio via DHCP server para todas as Unidades Distribuídas. A funcionalidade deverá ser gerenciada/configurada de forma centralizada no mesmo portal SD-WAN . Dentre os parâmetros necessários do DHCP server, estão os endereços de DNS primário e secundário, WINS e "scope options", de acordo com a solicitação do Banco. Atualmente, o Banco utiliza opções 246 e 248 com string de até 70 caracteres, por exemplo. A solicitação de configuração por parte do Banco não deverá representar custos adicionais ao projeto e deverá atender o SLA definido;

8.62 A solução deverá ser compatível com a implementação de Network Address Translation (NAT);

8.63 Garantir o funcionamento do tráfego de FTP entre as unidades distribuídas e o CAPGV, mesmo quando passar por NAT nos equipamentos fornecidos;

8.64 A solução deverá implementar funcionalidades de Access Control List (ACL) simples e estendidas ou similar com o objetivo de permitir e/ou bloquear tráfego informados pelo Banco;

8.65 A solução SD-WAN Central deverá implementar Agregação de links (802.3ad/LACP) para comunicação com os comutadores do BNB. A agregação poderá ser realizada diretamente pelos appliances ou por comutadores fornecidos com a solução nos cenários onde a distribuição dinâmica de carga entre interfaces ocorra via orquestração centralizada;

8.66 Em caso de falha ou degradação das métricas dos circuitos de comunicação, o tráfego deverá ser desviado automaticamente para outro link ativo e após resolução dos problemas, o retorno do tráfego deverá ser automático, ou seja, sem configuração manual;

8.67 A solução SD-WAN deve permitir a monitoração da latência, do jitter e do descarte de pacotes em cada um dos links individualmente e em cada direção (uplink/downlink) de forma independente;

8.68 A solução deverá implementar mecanismo de proteção contra variação de latência (jitter) ainda que a degradação seja em todos os links, para proteger o tráfego do tipo tempo real (voz e vídeo).

8.69 A solução deve ser capaz de monitorar e qualificar os links (em pelo menos dois níveis de qualificação);

8.70 A solução deve implementar MOS (Mean Opinion Score) ou recurso de avaliação de qualidade similar;

8.71 A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

- 8.71.1 Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente;
- 8.71.2 Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;

8.72 A solução SD-WAN deve ser capaz de utilizar todos os circuitos disponíveis na unidade distribuída e realizar balanceamento entre os links simultaneamente;

8.73 A solução deve permitir a verificação constante da situação dos links com o objetivo de identificar oscilações ou perdas destes, aplicando penalidades de forma automática, para não impactar os serviços e a experiência dos usuários;

8.74 Deve implementar solução de FEC (Forward Error Correction) nas conexões entre os appliances remotos e o datacenter, que possibilitem a redução da perda de pacotes na rede:

- 8.74.1 Tal funcionalidade deverá ocorrer em ambos os sentidos do tráfego;
- 8.74.2 Essa função pode ser substituída por duplicação de pacotes por caminhos distintos;

  8.74.2.1 No caso de duplicação de pacotes, a solução deverá garantir que os hosts não recebam pacotes duplicados;

  8.74.2.2 Deverá ser possível determinar em qual serviço o FEC ou duplicação de pacotes será habilitado.

8.75 A solução deverá ser capaz de criar Interfaces VLANs L3 e realizar o roteamento dessas redes e realizar a publicação via BGP dessas redes, se assim solicitado pelo Banco;

8.76 Implementar a criação de VLANs, permitindo:

- 8.76.1 Criar múltiplas VLANs, no mínimo 10;
- 8.76.2 Configurar a porta LAN da solução para suportar uma única VLAN (Porta de Acesso) ou múltiplas VLANs (Porta em Trunk);
- 8.76.3 Especificar uma subnet IP e associá-la à VLAN;
- 8.76.4 Configurar o appliance como o Gateway da VLAN;
- 8.76.5 Todas as VLANs deverão funcionar em contingência de gateway com o roteador MPLS conforme descrito em item anterior.
- 8.76.6 Permitir criar regras que impeçam a comunicação entre VLAN's na LAN das unidades distribuídas das quais o SD-WAN é o gateway;

8.77 A solução deverá ser capaz de definir políticas de engenharia de tráfego de forma centralizada com classificação do tráfego nos links disponíveis, utilizando pelo menos os seguintes critérios:

- 8.77.1 Com base em um único ou vários IPs;
- 8.77.2 Com base em uma única ou várias Subnet;
- 8.77.3 Com base em uma ou várias portas TCP/UDP;
- 8.77.4 Com base no valor do DSCP;
- 8.77.5 Com base na assinatura de aplicações conhecidas pela ferramenta SD-WAN.

8.78 A solução deve implementar controles de políticas de acesso por IP (origem e destino) porta (destino) e protocolo, inclusive nas redes locais onde o *appliance* SD-WAN estiver conectado.

8.79 Deve suportar a consulta a fontes externas de endereços IP, podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego (esta funcionalidade poderá ser atendida no SD-WAN ou no serviço SSE especificado no item 9).

8.80 A solução deverá ser compatível com as classes de QoS informadas na especificação dos circuitos de comunicação e roteadores do Edital;

8.81 A solução deverá alocar/especificar largura de banda do circuito de comunicação conforme a Classe e Nível de prioridade do tráfego;

8.82 A solução de SD-WAN deverá ser capaz de classificar e marcar os pacotes com DSCP (Differentiad Services Code Point), conforme as políticas definidas pelo Banco, para que os roteadores das operadoras contratadas possam dar a devida prioridade e banda necessária para cada tráfego, tanto do lado do datacenter (site principal e site secundário) como do lado das Unidades Distribuídas. Essa configuração deverá ser realizada de forma centralizada na solução de SD-WAN;

8.83 Para a comunicação via acessos MPLS, a solução de SD-WAN deverá também manter (ou alterar a critério do Banco) a marcação QoS nos casos informados pelo Banco. Será necessário, por exemplo, para manter o tráfego marcado com DSCP EF (VOIP) e AF41 (vídeo) na origem, de acordo com solicitação do Banco. Essa marcação será usada no processo de priorização dos circuitos MPLS na nuvem da operadora. No caso do tráfego destinado via link de internet, por indisponibilidade do link MPLS ou pela qualidade de link internet estar melhor, a marcação recebida pela rede interna deverá ser usada para priorização nas filas de transmissão de QoS da solução SD-WAN.

8.84 A solução deverá possuir a capacidade de classificar e visualizar o tráfego de rede para colocá-lo em uma das classes de serviço de acordo, com pelo menos os seguintes critérios:

- 8.84.1 Com base em um único ou vários IPs;
- 8.84.2 Com base em uma única ou várias Subnet;
- 8.84.3 Com base em uma ou várias portas TCP/UDP;
- 8.84.4 Com base no valor do DSCP;
- 8.84.5 Com base na assinatura de aplicações conhecidas pela ferramenta SD-WAN, no mínimo 1.100 aplicações (sendo no mínimo as aplicações Microsoft Office

365, Teams, Windows Update, Youtube, Facebook/Meta, Whatsup, google drive, instagram, Skype, Symantec, Outlook, p2p, acesso remoto, etc);

8.85 Deverá ser possível verificar, via sistema de gerenciamento, por qual caminho (qual circuito de comunicação) cada aplicação está trafegando. A solução deve ser capaz de fornecer visibilidade em todo o caminho (desde o Data Center até a Unidade Distribuída);

8.86 O tráfego deverá ser capturado, por exemplo, através de flows exportados diretamente dos equipamentos envolvidos nessa contratação, mas obrigatoriamente deve ser independente dos modelos de roteadores ou qualquer outro equipamento externo a solução contratada;

8.87 Deverá ser capaz de apresentar estatísticas de utilização das interfaces em ambos os sentidos, entrada e saída;

8.88 A solução SD-WAN deve permitir monitorar, no mínimo, os seguintes recursos:

- 8.88.1 Principais aplicativos/aplicações que estão usando mais largura de banda na WAN;
- 8.88.2 análise de partes da WAN com a latência mais alta em tempo real.
- 8.88.3 análise de perda média e máxima de pacotes em tempo real, em conjunto e em conexões WAN individuais.
- 8.88.4 identificação/quantificar pacotes que são entregues na WAN, em média e durante os períodos de pico;
- 8.88.5 informações de fluxo do usuário(ou endereço IP) em tempo real para solução de problemas;
- 8.88.6 visualização do túnel Overlay em tempo real para mostrar como vários transportes estão sendo usados pelas políticas de aplicativo
- 8.88.7 gráficos em tempo real que mostram o uso da largura de banda de diferentes classes de tráfego, como voz, vídeo, aplicativos de transferência de arquivos, etc.
- 8.88.8 visualização da latência no caminho WAN.

8.89 A solução deverá fornecer dados de Internet Protocol Flow Information eXport (IPFIX) ou Netflow ou equivalente tanto para o serviço de gerenciamento do NOC dessa contratação como para as ferramentas do Banco, se solicitado pelo Banco, sem custos adicionais. Atualmente, as ferramentas do Banco são do fabricante CA e o flow deve ser compatível com os produtos desse fabricante (Spectrum Version 10.2.1.0.98 e Network Flow Analysis 9.2.1);

8.90 As informações de relatórios de tráfego devem estar disponíveis por no mínimo 06 (seis) meses;

8.91 Implementar tecnologia para reconhecimento de aplicações e subaplicações (DPI - Deep Packet Inspection);

8.92 Para os Datacenters, a solução SD-WAN deverá suportar a capacidade de roteamento de tráfego (throughput), no mínimo de **30Gbps**;

- 8.92.1 Para os Datacenters, deverá possuir uma Solução de Firewall incorporado aos equipamentos de SD-WAN do mesmo fabricante, tanto para a solução instalada no Site Principal como no Site Secundário. A solução de firewall deverá possuir *throughput* compatível com o tráfego dimensionado para a solução de SD-WAN central, considerando uso dos recursos de visibilidade camada 7 do tráfego e criptografia dos túneis VPN;

8.93 Para dimensionamento da solução das Unidades Distribuídas, a título de roteamento de tráfego (*throughput*), suportar a soma dos links daquela Unidade, conforme **Anexo III - Endereços e Velocidades** do Edital, permitindo escalar o crescimento de 100% (cem por cento), sem a necessidade de troca do equipamento. Isto é, caso o somatório de larguras de banda de determinada localidade seja 320Mbps, o equipamento deverá suportar o tráfego WAN de pelo menos 640Mbps;

8.94 Nas Unidades Distribuídas, deverá possuir uma Solução de Firewall incorporado aos equipamentos de SD-WAN, do mesmo fabricante. A solução de firewall deverá possuir *throughput* compatível com o tráfego dimensionado para a solução de SD-WAN daquela unidade, considerando inclusive o crescimento mencionado acima, com o uso dos recursos de visibilidade camada 7 do tráfego e criptografia dos túneis VPN, não podendo ser nenhuma inferior a de 300Mbps.

8.95 O recurso de firewall dos appliances SD-WAN de cada unidade deverá implementar regras de liberações de acesso para Internet (breakout) a critério do BANCO. A replicação e ativação da regra/política deverá ser feita de forma automática após publicação centralizada. Deverá ser possível criar liberações de acesso para destinos, informando o endereçamento IP ou redes sumarizadas válidas na internet, domínio de internet (URL) por aplicação reconhecida pelo fornecedor de SD-WAN sendo no mínimo as aplicações Microsoft Office 365, Teams, Windows Update, Youtube, Facebook/Meta, Whatsup, google drive, instagram, Skype, Symantec, Outlook, p2p, acesso remoto, etc ;

8.96 Para as Unidades Distribuídas, a funcionalidade de firewall deverá realizar bloqueio de qualquer tráfego originado na Internet, sem que nenhuma publicação da rede do Banco seja possível para acesso externo. Somente deverá ser permitido nas Unidades Distribuídas tráfego via VPN (via Internet e via MPLS), ou seja, tunel VPN fechado entre os dispositivos SD-WAN parte desta solução, sendo a exceção, somente os tráfegos explicitamente liberados conforme regras acima descritas (breakout). O tráfego sem criptografia é aceito somente na falha do appliance de SD-WAN remoto, onde obrigatoriamente somente a rede MPLS será usada para trafegar informações;

8.97 A solução deverá suportar a quantidade de 200 sessões simultâneas por usuário, no mínimo. A quantidade mínima de usuários por unidade está disponível no Anexo III - Endereços e Velocidades;

8.98 Deverá permitir regras globais para controles de segurança de camada L4 - L7 para as Unidades Distribuídas;

8.99 Deverá permitir regras de controle de segurança baseado em Protocolos (TCP e UDP) para as Unidades Distribuídas;

8.100 Deverá permitir regras de controle de segurança baseado em IP e Porta de Origem e em IP e Porta de Destino, com a capacidade de implementação de máscaras de subnet de comprimento variável para as Unidades Distribuídas;

8.101 As regras deverão permitir bloquear ou liberar o tráfego com base em aplicações customizadas pelo administrador, sendo que deverá ser possível fazer a definição com base nos critérios mínimos, abaixo relacionados:

- 8.101.1 Com base em um único ou vários IPs;
- 8.101.2 Com base em uma única ou várias Subnet;
- 8.101.3 Com base em uma ou várias portas TCP/UDP;
- 8.101.4 Com base na assinatura de aplicações conhecidas pela ferramenta SD-WAN;

8.102 A solução SD-WAN deverá implementar a infraestrutura de chave pública (PKI), de forma integrada, usando a autoridade de certificação (CA) ou através de uso do *pre-shared key* para troca de chave entre o appliances;

8.103 A solução deverá ser capaz de suportar para fechamento dos túneis criptografados:

- 8.103.1 Autenticação via Pre-Shared Key ou Certificado Digital X.509;
- 8.103.2 Suportar os protocolos IKE versões 1 e 2 para troca de chaves;
- 8.103.3 Deve suportar os algoritmos de criptografia AES-128 e AES-256;
- 8.103.4 Deve suportar, no mínimo, dois tipos de Algoritmos de Hash (MD5, SHA1, SHA256);
- 8.103.5 Deve suportar os Grupos de Diffie–Hellman Group14 (2048 Bits) e Group 19 (256 Bits eliptic curve);

8.104 A solução deverá possuir recursos de proteção, no mínimo contra os seguintes tipos de ataques:

8.104.1 Denial-of-Service (DoS)
8.104.2 TCP-based attacks : Invalid TCP Flags, TCP Land, e TCP SYN Fragment
8.104.3 ICMP-based attacks: ICMP Ping of Death e ICMP Fragment
8.104.4 IP Unknown Protocol

8.105 A contingência da solução SD-WAN deve ocorrer em âmbito local e global. Todas as necessidades de hardware (incluindo comutadores) e software (incluindo protocolos) necessários para a redundância e alta disponibilidade da solução exigidas nessas especificações devem ser fornecidas pela solução contratada;

8.106 Cada solução SD-WAN instalada nos datacenters (Site Principal e Site Secundário) deverá possuir redundância N+N e alta disponibilidade para todos os componentes em cada datacenter, de forma que quaisquer indisponibilidades em N-equipamentos SD-WAN sejam chaveadas automaticamente em até 3 (três) minutos sem perda de performance, dentro do mesmo datacenter inicialmente, após esse período. Enquanto a solução estiver funcionando em contingência, haverá apuração de SLA de disponibilidade;

8.107 Em âmbito global, cada unidade distribuída deve possuir concentração para 2 (dois) sites concentradores/datacenters funcionando em modo ativo-ativo ;

8.108 A solução SD-WAN das Unidades Distribuídas deverá implementar alta disponibilidade para, pelo menos, o circuito primário MPLS. Em caso da falha de um equipamento SD-WAN, o circuito primário MPLS deverá continuar ativo e em funcionamento, de maneira totalmente automática e transparente para o usuário, isto é, sem intervenção manual, podendo a solução utilizar protocolos de alta disponibilidade, como VRRP (Virtual Router Redundancy Protocol) disponibilizados pelos roteadores do ITEM 1 (desde que aderentes aos requisitos do item 1.5 do Anexo X- REQUISITOS DE GERENCIAMENTO DOS SERVIÇOS), ou bypass em hardware, especificamente para o circuito primário MPLS ou ainda prover appliances SD-WAN (N+1) com alta disponibilidade que sejam compatíveis com as especificações dos roteadores e topologia do Banco descritas no Edital. Para a alta disponibilidade, todas as necessidades físicas (como cabos, interfaces ou mesmo outros switches ou roteadores com portas "gigabit") e de software (por exemplo, protocolos e licenças) capazes de manter a alta disponibilidade deverá ser fornecidas em conjunto com a solução contratada;

8.109 Nas Unidades Distribuídas, em caso de indisponibilidade dos equipamentos do serviço SD-WAN, a solução deverá ainda bloquear todo e qualquer tráfego originado e/ou destinado diretamente à Internet. A falha do serviço de SD-WAN deverá indisponibilizar a comunicação direta com a Internet na unidade remota, inclusive em nível de camada 2 do modelo de referencia OSI, sem prejuízo do chaveamento do tráfego para o circuito MPLS, conforme já descrito;

8.110 Durante a implantação da Solução SD-WAN e durante a falha de equipamentos, na vigência do Contrato, a solução implantada deverá permitir que sites que já possuem a nova solução SD-WAN continuem se comunicando com os sites que ainda não a possuem (ou que estejam em contingência, via comunicação MPLS);

8.111 Nas Unidades Distribuídas, caberá ao Banco o fornecimento de conectividade camada 2 (sem roteamento) entre a rede corporativa do Banco e os appliances da nova solução. A solução contratada deverá ser compatível com 802.1Q (passagem de VLANs) no caso de VLANs criadas nos roteadores da operadora MPLS. Atualmente, o Banco possui segmentação lógica para redes de videoconferência, por exemplo;

8.112 É de responsabilidade da solução contratada implementar recursos para identificar e proteger os equipamentos SD-WAN de todo e qualquer tráfego interno a partir da unidade remota do Banco, seja por tempestades de broadcast, unicast, multicast ou por qualquer outro motivo. Todo problema interno na unidade não deverá ser replicado para outras redes do Banco. As unidades do Banco não possuem outros equipamentos L3 configurados além dos aqui contratados, diversas redes do Banco são "/16" e com endereçamentos válidos, porém não publicados para internet;

8.113 Em caso de falha em um dos sites do Banco o chaveamento do tráfego deverá ocorrer entre os Sites do BANCO (Site Primário <-> Site Secundário), via roteamento dinâmico e sem intervenção manual;

8.114 Roteamento dinâmico implementado na LAN do CAPGV entre concentradores e roteador gateway. O protocolo de roteamento na LAN do CAPGV será definido pelo Banco durante implementação, atualmente é via BGP.

8.115 Deverá ser oferecido Treinamento de Operação de toda a solução SD-WAN ofertada com carga mínima de 40h, sendo esse ministrado nas dependências do CAPGV 4h por dia e contemplando no mínimo 1 turma de até 15 pessoas presenciais e outras 10 pessoas transmitindo remotamente via Teams onde será gravado pelo Banco do Nordeste como forma de treinamento e documentação para os profissionais internos. O treinamento deverá ser ministrado durante ou imediatamente após a implantação, a critério do Banco, pelo CONTRATADO ou por empresa contratada por este;

8.116 A instalação e configuração da solução ofertada é de responsabilidade da CONTRATADA, bem como toda a conexão de cabos e demais necessidades envolvidas na solução entregue, incluindo a conexão entre os roteadores dos circuitos de dados (primários, secundário e terciários) com a solução SD-WAN e a rede do Banco, de forma a causar o menor impacto possível nas migrações e manter os requisitos de segurança e disponibilidade exigidos no Edital, onde é fundamental que a conexão com qualquer circuito de internet seja realizada fisicamente passando pelo appliance de SD-WAN, por exemplo:

8.116.1 Caso a solução de SD-WAN seja instalada na Unidade Distribuída antes da instalação dos novos circuitos de comunicação (**ITEM 1**), a mesma deverá ser instalada utilizando os atuais circuitos de comunicação para encaminhamento do tráfego. Caberá ao vencedor desse item acompanhar com o NOC de gerenciamento, mesmo que de forma remota, toda a conexão dos novos circuitos de dados com a rede do Banco, mantendo os requisitos de segurança solicitados no Edital, inclusive durante período de migração/implantação;

8.116.2 Caso a solução de SD-WAN seja instalada depois dos novos circuitos de dados (**ITEM 1**), caberá ao contratado do **ITEM 2** a conexão entre a solução de SD-WAN com os novos circuitos (**ITEM 1**), bem como com a rede do Banco. No momento da migração, já será de responsabilidade do NOC contratado o acionamento da operadora para resolução de problemas de circuito de comunicação, seja relacionado com configuração ou com a ativação do mesmo;

8.116.3 O Banco se responsabilizará pela disponibilização de racks ou bancadas para instalação (caso não disponha de espaço no rack) e da infraestrutura elétrica necessária, tais como réguas e pontos de energia;

8.116.4 Caberá ao Banco o agendamento da instalação inicial com as suas Unidades e com as CONTRATADAS dos ITENS 1 e 2, de acordo com o cronograma definido pelas CONTRATADAS dos ITEMS 1 e 2.

8.117 A solução SD-WAN deverá ser capaz de permitir integração segura entre unidades distribuída e plataformas SaS (Software as Service) de outros fabricantes, de forma a diminuir a latência na comunicação e aumentar o desempenho das aplicações.

8.118 A solução deve oferecer suporte à integração com a solução SSE ofertada para segurança avançada na Internet.

9 REQUISITOS GERAIS DA SOLUÇÃO DE SECURITY SERVICE EDGE (SSE) (ITEM 2)

9.1 A solução de segurança na borda deverá suportar, no mínimo, as seguintes funcionalidades:

- 9.1.1 Filtro de URL;
- 9.1.2 Controle de Aplicação;
- 9.1.3 Proteção Contra Malwares Modernos;
- 9.1.4 Prevenção de Ameaças;
- 9.1.5 ZTNA (Zero Trust Network Access).

9.2 A solução deverá ser disponibilizada numa arquitetura em nuvem;

9.3 A solução disponibilizada deverá ter capacidade de receber via redirecionamento ou interceptar de maneira ativa e realizar inspeção e tratamento de todo o tráfego web de forma a controlar os acessos a serviços SaaS (Gerenciados e não gerenciados), IaaS, Web e Aplicações Internas (Nuvem pública ou *on-premises*);

9.4 A solução deverá ser fornecida como SaaS (Software as a Service) em ambiente externo ao Banco. Isto é, não serão permitidas soluções de segurança do tipo *on-premises*.

9.5 A solução deve possuir console de gestão web para toda a plataforma de segurança, incluindo:

- 9.5.1 Painel de Política;
- 9.5.2 Painel de Relatório;
- 9.5.3 Painel de Incidentes;
- 9.5.4 Painel de Configuração;
- 9.5.5 Painel Analítico.

9.6 O fabricante da solução deverá possuir ao menos 2 (dois) gateways no Brasil, não sendo permitidas soluções genéricas agregadas através de appliances físicos e/ou virtuais;

9.7 Todo o processamento do tráfego deverá ser realizado em Datacenters localizados no Brasil;

9.8 A solução deverá prover às redes remotas faixas de endereços exclusivos para acesso à Internet, saindo apenas com IPs designados para o fabricante da solução SSE e alocados no Brasil.

9.9 A solução deverá garantir SLA de latência para, no mínimo, as aplicações do Microsoft Office 365 ou possuir *peering* estabelecendo conexão direta entres os POPs do fabricante SSE e o Datacenter da Microsoft no Brasil;

9.10 A infraestrutura operacional do fabricante da solução deverá ter as certificações SOC-2 e ISO 27001;

9.11 Deverá ser possível realizar a interceptação do tráfego de várias maneiras distintas, com o intuito de cobrir todo o escopo de alcance aos usuários, para no mínimo as seguintes formas:

9.11.1 Túnel Seguro (IPSEC ou SSL);

9.11.2 Integração com a Plataforma de SDWAN ofertada;

9.11.3 Integração com NGFW/UTM (IPSEC);

9.11.4 Agente (Windows e MacOS);

9.12 Os serviços de segurança devem ser fornecidos de maneira transparente às redes remotas;

9.13 A solução deve fornecer a capacidade de associar e atribuir toda a atividade do usuário, usando uma representação de identidade conforme integrações com:

9.13.1 *Azure Active Directory*;

9.13.2 Federação (SSO) utilizando SAML v2.0.

9.14 Suportar recurso de autenticação única para todo o ambiente de rede da CONTRATANTE, utilizando a plataforma de autenticação *Active Directory* ou outra plataforma com suporte à SAML;

9.15 A solução deverá executar suas funcionalidades em defender a rede contra ameaças avançadas, vírus e ameaças escondidas em tráfego HTTPS e aplicações com SSL criptografado;

9.16 A solução deverá ser capaz de descriptografar e inspecionar todo o tráfego SSL/TLS, nas versões TLS 1.2 ou superior;

9.17 O tráfego SSL/TLS deve ser inspecionado pelas mesmas políticas de filtragem aplicadas ao tráfego não criptografado;

9.18 A solução deverá suportar e estar devidamente licenciada para:

9.18.1 No mínimo a quantidade de **12.000 (doze mil)** usuários autenticados com serviços ativos e identificados pela solução;

9.18.2 Até a quantidade de **10 (Dez) Gbps** de troughput para todos as funcionalidades ativas simultaneamente, conforme **Anexo II – Modelo de Proposta**;

9.18.3 A solução de ***ZTNA (Zero Trust Network Access)*** deverá suportar pelo menos **12.000 (doze mil)** usuários, sendo até **4.000 (quatro mil) simultâneos**, conforme **Anexo II – Modelo de Proposta**;

9.18.4 No mínimo a quantidade de dispositivos informada no **Anexo II – Modelo de Proposta**, identificados pela solução.

9.19 A solução deverá possibilitar a execução de descriptografia SSL para todo o tráfego WEB, e deverá ser escalável para suportar ao longo do contrato a quantidade total de usuários licenciados;

9.20 Deverá permitir a configuração de portas diferentes da porta padrão utilizada pelos protocolos HTTPS/SSL e HTTP, utilizado no acesso de clientes a sites;

9.21 A solução deverá verificar os certificados digitais de sites acessados por meio do protocolo HTTPS. Em caso de certificados digitais inválidos, a solução deverá ser configurável para, de acordo com preferência da CONTRATANTE, bloquear ou permitir o acesso aos sites;

9.22 Deverá permitir configurar regras de exceção a sites HTTPS que não devem ter seu tráfego inspecionado;

9.23 A solução deverá ser capaz de se integrar com a solução de SD-WAN ofertada;

9.24 O licenciamento e a garantia pelo fabricante para toda a solução deverão estar ativos durante toda a vigência do contrato;

Filtro de URLs

9.25 A solução deverá suportar a criação de políticas baseadas no controle por URL e categorias de URLs;

9.26 O perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação;

9.27 A solução deverá possuir:

9.27.1 Pelo menos 70 categorias distintas de URLs;

9.27.2 A capacidade de classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;

9.27.3 Categoria específica para classificar domínios recém registrados;

9.27.4 Base contendo, no mínimo, 20 milhões de sites internet web já registrados e classificados com atualização automática, possuindo, ainda, interface complementar disponibilizada pelo fabricante para inclusão e sugestão de alteração de classificação de URL;

9.28 A solução deve possuir, no mínimo, os seguintes atributos para construção de políticas na plataforma:

9.28.1 Categoria de URL;

9.28.2 Usuários e Grupos do Active Directory;

9.28.3 Profile de prevenção de malwares, podendo ser definido de forma global ou por política de acesso;

9.28.4 Atividade realizada na URL/Aplicação;

9.28.5 IP de Origem;

9.28.6 Ação: allow e block;

9.28.7 Tipo/extensão de arquivo.

9.29 A categorização de URL deverá analisar toda a URL e não somente até o nível de diretório;

9.30 A solução deverá suportar:

9.30.1 A criação de categorias de URLs customizadas;

9.30.2 A exclusão de URLs do bloqueio, por categoria;

9.30.3 A customização de página de bloqueio;

9.30.4 Rastreamento de sites e análise em, no mínimo, 40 idiomas;

9.30.5 Identificação e categorização de sites acessados através de tradutores (ex. Google Translate);

9.30.6 A capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local.

9.31 A solução deverá permitir:

9.31.1 Um mecanismo para sobrescrever as categorias de URL;

9.31.2 A criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra);

9.31.3 Especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

9.32 A solução deverá possuir mecanismo de Controle de URL que apresenta contagem de utilização de regra de acordo com a utilização (*hit count*);

9.33 A solução deverá possibilitar:

9.33.1 Categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente;

9.33.2 A inspeção de tráfego HTTPS *Outbound* deverá efetuar o "*man-in-the-middle*", ou seja, a solução deverá prover mecanismo de descriptografia para inspeção completa do tráfego de saída para a internet;

9.33.3 Implementação de filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das estações dos clientes da COTRATANTE.

9.33.4 O cadastro manual de usuários e grupos diretamente na interface de gerência remota;

9.33.5 O bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);

9.33.6 Salvar nos logs, no mínimo, as informações do campo *UserAgent* do cabeçalho HTTP nos acessos a URLs;.

9.34 A solução deverá utilizar modelos de inteligência preditiva no reconhecimento de URLs maliciosas em tempo real não cadastradas na base de categorização do fabricante da solução.

9.35 A solução deverá possuir a capacidade de detectar técnicas de *phishing* ou falsificação de imagens;

Controle de Aplicação

9.36 A solução deverá possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

9.37 A solução deverá contar com módulos de visibilidade e controle que permitam administrar o tráfego de aplicações, permitindo o tráfego de aplicações autorizadas e bloqueio de aplicações não autorizadas;

9.38 Pela solução deverá ser possível:

9.38.1 A liberação e bloqueio somente das aplicações sem a necessidade de liberação de portas e protocolos;

9.38.2 Adicionar políticas de controle de aplicações e perfis de segurança para todo o tráfego web direcionado para a nuvem SSE, não se limitando somente a possibilidade de habilitar controle de aplicações em parte do tráfego;

9.38.3 A criação de políticas por geolocalização, permitindo que o tráfego de uma aplicação para um determinado país seja bloqueado ou redirecionado;

9.38.4 A criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

- Nível de risco da aplicação;
- Categoria de aplicações.

9.39 A solução deverá reconhecer pelo menos 3.000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a *peer-to-peer*, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e webmail;

9.40 A solução deverá suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos assinaturas, decoders de protocolos e heurísticas;

9.41 A solução deverá diferenciar:

9.41.1 Tráfegos *peer-to-peer* (*bittorrent*, *emule*, *neonet*, etc.), permitindo o bloqueio desse tipo de tráfego;

9.41.2 Aplicações proxies (ultrasurf, ghostsurf, freegate, etc.) permitindo o bloqueio desse tipo de tráfego;

9.41.3 Tráfegos de mensageiros instantâneos (facebook Chat, WhatsApp, telegram e etc.) possuindo granularidade de controle para os mesmos;

9.42 A solução deverá diferenciar e controlar partes das aplicações, incluindo, mas não limitado: Permitir o WhatsApp WEB e bloquear a transferência de arquivos, permitir o facebook e bloquear chat;

9.43 Pela solução deverá ser possível:

9.43.1 Inspecionar o *payload* do pacote de dados com o objetivo de detectar, através de expressões regulares, assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

9.43.2 Aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a *encrypted bittorrent* e aplicações VOIP que utilizam criptografia proprietária.

9.44 Caso a solução não tenha assinaturas pré-definidas de uma aplicação, a mesma deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP e HTTPS;

9.45 Pela solução deverá ser possível atualizar a base de assinaturas de aplicações automaticamente;

9.46 O fabricante da solução deverá disponibilizar um serviço para solicitação de inclusão de aplicações na base de assinaturas do mesmo;

Proteção Contra Malwares Modernos

9.47 A solução deverá possuir nuvem de inteligência onde seja responsável em atualizar toda a base de segurança através de assinaturas;

9.48 A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real;

9.49 A solução deve ser capaz de enviar arquivos trafegados de forma automática para análise, devendo permitir a análise na nuvem do fabricante da solução, onde o arquivo será executado e simulado em ambiente controlado (*sandbox*). Caso esta funcionalidade seja licenciada de forma separada da solução, deverão ser fornecidas todas as licenças necessárias para a utilização desta funcionalidade.

9.50 A solução deverá prevenir o uso de *exploits* avançados;

9.51 Na solução, a análise deverá prover:

9.51.1 Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

9.51.2 Informações sobre as ações do Malware na máquina infectada;

9.51.3 Informações sobre as URLs não confiáveis utilizadas pelo novo Malware;

9.51.4 Informações sobre quais aplicações são utilizadas para causar/propagar a infecção;

9.51.5 Detecção de aplicações não confiáveis, utilizadas pelo Malware;

9.51.6 Atualização das assinaturas de Antivírus e Antispyware de maneira automática na plataforma SSE.

9.52 A solução deverá possuir:

9.52.1 Antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP e HTTPS;

9.52.2 Mecanismo de detecção *antibot*, que inclui pelo menos, reputação de endereço IP;

9.52.3 Funcionalidade de detecção e bloqueio de *call-backs*.

9.53 A solução deverá prevenir contra ameaças de dia zero:

9.53.1 Via tráfego de internet;

9.53.2 Que possam burlar o sistema operacional emulado;

9.53.3 Através de tecnologias em nível de emulação e código de registro.

9.54 A solução deverá ser capaz de implementar:

9.54.1 Detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve permitir inspecionar arquivo PDF com até 2MB (dois MegaBytes);

9.54.2 Visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (*sandbox*) suportados;

9.54.3 Análise de arquivos executáveis, DLLs e ZIP em SSL no ambiente controlado;

9.55 A solução deverá permitir ainda:

9.55.1 Identificação e bloqueio de malware nas comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

9.55.2 Análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) no ambiente controlado;

9.55.3 Submissão manual de arquivos para análise através do serviço de *Sandbox*.

9.56 A solução deve permitir a criação de *Whitelist* baseado no *hash* do arquivo;

Prevenção de Ameaças

9.57 A solução deverá proteger o acesso do usuário aos dados corporativos, controlando a exposição dos mesmos quanto à movimentação entre nuvens (SaaS Gerenciado e SaaS não gerenciado);

9.58 Na solução deverá ser possível criar políticas de segurança baseadas no nível de risco da aplicação. Ex: selecionar na política de segurança o bloqueio de todas as aplicações de *cloud storage* com nível de risco alto na base do fabricante da solução;

9.59 Deve conter, no mínimo, as seguintes informações sobre as aplicações comparadas na interface gráfica da solução:

9.59.1 Informações sobre vulnerabilidades e *exploits* já sofridos;

9.60 A solução deverá possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou referentes a incidentes de vírus e Bots;

9.61 A solução deverá suportar referência cruzada com CVE;

9.62 A solução deverá ser capaz de categorizar os seguintes tipos de domínio:

9.62.1 Domínios de DNS dinâmicos;

9.62.2 Domínios identificados previamente como sendo distribuidores de *Malwares*;

9.62.3 Domínios identificados anteriormente em campanhas de *Phishing*;

9.62.4 Domínios identificados previamente como *Graywares* os quais podem usar de técnicas de instalação de aplicações não desejadas;

9.62.5 Domínios Estacionários os quais são sites com conteúdo limitado e que podem ser utilizados como um ponto de distribuição de malwares;

9.62.6 Domínio de anonimização de Proxy utilizados com uma forma de driblar a análise de conteúdo.

9.63 Os requisitos abaixo descritos neste item poderão ser atendidos pela solução SSE ou pela solução SDWAN ofertada:

9.63.1 A solução deverá possuir sistema de análise automática para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

9.63.2 A solução deve proteger contra ataques do tipo envenenamento de cache DNS (*DNS Cache Poisoning*), e impedir que os usuários acessem endereços de domínios bloqueados ou maliciosos;

9.63.3 A solução deverá permitir *updates* em tempo real para ameaças e novos ataques feitos através de DNS.

ZTNA (*Zero Trust Network Access*)

9.64 A solução deve possuir a capacidade de controlar o acesso e aplicar Controle de Aplicação, Proteção Contra Malwares Modernos e Prevenção de Ameaças, de usuários remotos a aplicações internas da CONTRATANTE através da nuvem do fabricante, onde o usuário remoto tenha acesso apenas a aplicação especificada na política de segurança e não a um segmento de rede interna;

9.65 A solução deve ser implementada com agente único na estação de trabalho do usuário remoto;

9.66 A solução deve garantir acesso seguro a nível de aplicação, ao invés de prover acesso local a rede;

9.67 Ser possível configurar através da console gráfica da solução quais aplicações internas serão acessadas através do *Tenant* da solução;

9.68 Ser autossuficiente e se ajustar automaticamente do ponto de vista de performance caso algum ponto de presença venha a falhar sem a necessidade do administrador ou cliente configurar nenhuma regra;

9.69 Trabalhar em modo híbrido onde seja possível publicar os atalhos de acesso a aplicações presentes nos datacenters da CONTRATANTE e nas nuvens públicas indicadas pela mesma;

9.70 A solução deve permitir definir a conformidade de estações com sistemas operacionais Windows e MacOS, com as políticas organizacionais baseadas no mínimo nos seguintes critérios:

9.70.1 Presença de processo(s) em execução;

9.70.2 Presença de arquivos em disco;

9.70.3 Participação em domínio do AD;

9.70.4 Existência de Certificado Digital no dispositivo;

9.70.5 Que somente as máquinas que estejam com solução antimalware ativada possam acessar os serviços internos.

9.71 A solução deverá permitir o acesso diferenciado para um mesmo usuário conforme as seguintes condições:

9.71.1 Máquinas em conformidade: A partir de uma máquina remota, com pré-requisitos de segurança identificados, deve permitir o acesso a aplicação;

9.71.2 Máquinas não conformes: A partir de uma máquina remota, uma estação que não atenda aos requisitos de segurança, deve bloquear o acesso a aplicação.

9.71.3 Geolocalização: A partir de uma máquina remota tentando se conectar de um país não permitido, deverá ter sua conexão bloqueada.

9.72 Pela solução deve ser possível criar políticas de segurança onde pode ser especificado:

9.72.1 Usuário do AD;

9.72.2 Grupo do AD;

9.72.3 Aplicação Privada;

9.72.4 Perfil de segurança (por exemplo: Filtro de URLs e Controle de Aplicação);

9.72.5 Ação: Permitir e/ou Bloquear.

9.73 A solução deve realizar verificação contínua de confiança, onde uma vez que o acesso a um aplicativo é concedido:

9.73.1 A Confiança deverá ser continuamente avaliada com base em mudanças nas condições de segurança na estação;

9.73.2 Se algum comportamento suspeito for detectado, o acesso pode ser revogado em tempo real;

9.74 A solução deve gerar logs dos acessos realizados por usuários remotos as aplicações internas, no mínimo, com as seguintes informações:

9.74.1 Regra de segurança que foi aplicada no tráfego;

9.74.2 Ação tomada pela solução;

9.74.3 Usuário;

9.74.4 Endereço IP;

9.74.5 País de origem;

9.74.6 Porta de origem;

9.74.7 Sistema operacional;

9.74.8 Aplicação de destino;

9.74.9 Porta de destino;

9.74.10 Protocolo;

9.74.11 Bytes tráfegados na sessão;

9.74.12 Hora de início e término da sessão.

Relatórios

9.75 Ser capaz de visualizar, de forma direta na solução, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados, URLs acessadas e ameaças identificadas;

9.76 Ser capaz de visualizar, de forma direta na solução, o *throughput* de dados utilizado pela rede de computadores conectados ao serviço em nuvem. Esse requisito poderá ser atendido pela solução SSE ou pela solução SDWAN ofertada;

9.77 Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar tráfego de arquivos maliciosos, dentre outras ameaças. Deve permitir o download do relatório em formato PDF;

9.78 Ser capaz de visualizar, de forma direta na solução, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização;

9.79 Possibilitar a geração de, pelo menos, os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web);

9.80 A contratada deverá disponibilizar, no mínimo, 365 dias de retenção de dados para disponibilizar relatórios. Os relatórios devem ser disponibilizados atendendo aos seguintes critérios:

9.80.1 No mínimo 30 dias na própria console da solução de SASE/SSE;

9.80.2 No mínimo 12 (doze) meses, podendo ser na própria console da solução de SSE ou em uma solução externa ao ambiente SSE, contanto que forneça, no mínimo, os seguintes formatos de relatórios:

- Relatório de acesso a internet por usuário, contendo as informações de data, hora, URL destino, categoria da URL, regra de acesso e aplicação;
- Relatório de acesso a internet por URL destino, contendo as informações de usuários e categoria da URL;
- Relatório de acesso a internet por Aplicação, contendo as informações de usuários;

Gerenciamento

9.81 Deve ter administração por console de gerenciamento web para toda a plataforma SSE, incluindo os recursos abaixo listados:

9.81.1 Filtro de URL;

9.81.2 Controle de Aplicação;

9.81.3 Proteção Contra Malwares Modernos;

9.81.4 Prevenção de Ameaças;

9.81.5 ZTNA (Zero Trust Network Access).;

9.82 O gerenciamento da solução deverá ser baseado em plataforma WEB, com acesso via browser padrão de mercado, utilizando comunicação criptografada (TLS, versão 1.2 ou superior);

9.83 A solução deverá ter a capacidade para criação das contas de usuário na própria console de gerenciamento com diferentes níveis de acesso, para no mínimo, administração e operação.

9.84 A solução deverá ter a capacidade de utilizar contas de usuários do AD interno do Banco para autenticação na console de gerenciamento, através de integração com o *Azure Active Directory*;

9.85 A solução deve estar licenciada e permitir o uso de duplo fator de autenticação (2FA ou MFA) para acesso à console de administração da solução. Caso a solução necessite de mais de uma console de gerenciamento, todas devem estar licenciadas e permitir o uso do MFA;

10 INTEGRAÇÃO DO TRÁFEGO DE DADOS, VOZ E IMAGENS (SD-WAN e acessos MPLS) (exceto Parceiros)

10.1 Definição de classes de tráfego

10.1.1 Deverão ser criadas diferentes classes de tráfego em quantidade e com características que permitam a perfeita integração, numa mesma infraestrutura, do tráfego de dados, voz e imagens entre as unidades distribuídas e o CAPGV, de modo a atender os requisitos apresentados.

10.2 Classificação do tráfego

10.2.1 O tráfego de dados, voz e imagens gerado pelos diferentes sistemas do Banco instalados nas unidades distribuídas, no Site Primário e Site Secundário deverá ser adequadamente classificado, priorizado, encaminhado e entregue pelos equipamentos fornecidos no escopo dos serviços do ITEM 2 (SD-WAN), de modo a garantir o perfeito funcionamento dos respectivos sistemas. Isso deve ser feito respeitando os critérios de priorização de cada classe de tráfego, conforme indicado nos itens abaixo.

10.2.2 A CONTRATADA do **ITEM 1**, de acessos MPLS, deverá garantir que os pacotes marcados pela solução SD-WAN, vindos do Banco, serão garantidos dentro dos seus backbones de acordo com os percentuais e classes estabelecidos nos itens referentes à Alocação de Classes e Alocação de Banda, deste Edital, sem que haja qualquer remarcação, incluindo para o tráfego entre unidades distribuídas diferentes, ou seja, dentro do perfil de tráfego full mesh.

10.3 Capacidade de transmissão para tráfego de voz

10.3.1 Os serviços prestados pelo CONTRATADA do **ITEM 1** . para fornecimento MPLS deverão implementar os recursos necessários, incluindo controle do retardo máximo, controle da variação do retardo, quebra do tamanho de pacotes, compressão de cabeçalho RTP, mecanismos de fragmentação e interleaving (LFI), dentre outras funcionalidades, de modo a garantir o perfeito funcionamento das chamadas de voz entre as centrais telefônicas.

10.4 Tráfego de imagens

10.4.1 A rede de serviços integrados deverá interligar os sistemas de videoconferência instalados nas unidades distribuídas, Site Secundário e no Site Primário, permitindo o estabelecimento de chamadas de videoconferência, incluindo som e imagem, para cada unidade distribuída, tendo como destino uma outra unidade distribuída, Site Secundário ou o Site Primário. Os sistemas de videoconferência instalados nas unidades distribuídas, Site Secundário e no Site Primário já estão equipados com interfaces para transformação dos sinais de som e imagens e seus respectivos protocolos em pacotes tipo Internet Protocol (IP). Tais interfaces deverão ser interligadas aos comutadores de rede locais nas unidades distribuídas, Site Secundário e no Site Primário. A interligação dos sistemas de

videoconferência aos equipamentos comutadores das redes locais das unidades distribuídas, Site Secundário e do Site Primário, bem como as necessárias configurações nesses mesmos sistemas de videoconferência, são de responsabilidade do Banco, estando fora do escopo dos serviços ora especificados.

10.5 Capacidade de transmissão para tráfego de videoconferência

10.5.1 Os serviços prestados pelo CONTRATADA **do ITEM 1**. deverão implementar os recursos necessários, incluindo controle do retardo máximo, controle da variação do retardo, quebra do tamanho de pacotes, dentre outras funcionalidades, de modo a garantir o perfeito funcionamento das chamadas entre os sistemas de videoconferência atualmente em uso pelo Banco. De acordo com especificações do fabricante dos sistemas de videoconferência, cada chamada de videoconferência poderá requerer pelo menos 512Kbps de capacidade de transmissão para seu efetivo funcionamento, incluso o overhead do protocolo IP.

10.6 Unidades envolvidas

10.6.1 Todas as unidades distribuídas poderão dispor de recursos para realização de videoconferência, e deverão, portanto, ter seus serviços devidamente preparados para tal. Quaisquer alterações ou inclusões de novas unidades serão solicitados ao CONTRATADA a qualquer momento, sem ônus para o Banco.

10.7 Tráfego de dados

10.7.1 O tráfego de dados (exceto voz e vídeo) entre as unidades distribuídas e o CAPGV deverá ser diferenciado em 3 níveis de prioridade além do Best Effort (BE), a saber: alta (mission critical), média (transactional) e baixa (bulk data). Em cada nível de prioridade deverá ser permitido até 3 grupos de classificação com diferentes probabilidades de descarte, como por exemplo, no nível AF2, será permitida a marcação AF21, AF22 e AF23. Os dados classificados como de alta prioridade deverão ser encaminhados, até o limite pré-estabelecido, com prioridade sobre os dados classificados como de média prioridade, que por sua vez deverão ser encaminhados, até o limite pré-estabelecido, com prioridade sobre os dados classificados como de baixa prioridade. O tráfego relacionado aos serviços de voz e imagens deverá ter prioridade sobre todas as classes de dados, de modo a garantir o perfeito funcionamento e integração de todos os serviços. Conforme mencionado abaixo nesse anexo, deverá ser permitido o transbordo de dados entre as classes, conforme será informado pelo Banco durante implantação.

10.8 Interoperabilidade entre as operadoras

10.8.1 O CONTRATADA **do ITEM 1** deverá garantir a interoperabilidade entre o tráfego de agências distintas de forma transparente ao Banco, utilizando a infraestrutura de roteadores e comutadores instalados por cada operadora no Site Primário e Site Secundário como meio de interconexão física entre suas redes MPLS. Tal interoperabilidade deverá ser assegurada através de configuração nos equipamentos da operadora, que funcionarão como gateways, atendendo a seguinte definição das classes de serviço em seus backbones:

Mapeamento das Classes de Serviços

Tráfego de Voz		Classe EF
Tráfego de Imagem		Classe AF4
Tráfego de Dados	Alta	Classe AF3
	Média	Classe AF2
	Baixa	Classe AF1

10.8.2 De acordo com as prioridades do tráfego definidas pelo Banco, os critérios acima deverão ser obedecidos pelas operadoras, seguindo os padrões descritos nas RFCs 2474 e 2475 – DiffServ, complementados pela RFC 2597 – Assured Forwarding Per-hop Behaviors (AF PHB) e pela RFC 2598 – Expedited Forwarding (EF).

10.8.3 Os serviços prestados pela operadora deverão permitir a criação de VPN (Virtual Private Network) através de MPLS (Multiprotocol Label Switiching), construída de acordo com a RFC 2547 e a RFC 3031. Também deverá ser garantida a configuração de QoS (Quality of Service) sobre MPLS/VPN, de acordo com a RFC 3270 e a RFC 2983.

10.8.4 O tráfego de voz deverá ser mapeado para a classe EF e o tráfego de imagem deverá ser mapeado para a classe AF4. O tráfego de dados de alta prioridade, média prioridade e baixa prioridade deverão ser mapeados respectivamente para as classes AF3, AF2 e AF1.

10.8.5 A soma da porcentagem de reserva de cada circuito de dados será informada pelo Banco durante implementação e poderá sofrer alteração durante todo o Contrato, de acordo com solicitação do Banco. A soma da porcentagem de todas as classes não passará de 96%, ficando livre para a operada até 4% do acesso para utilização de tráfego de gerência que será especificado, configurado e mantido pela própria operadora.

10.9 Alocação de Largura de Banda

10.9.1 A caracterização das três classes de dados (alta, média e baixa), da classe de voz e da classe imagem deverá seguir a associação definida nas tabelas abaixo:

Alocação de Largura de Banda					
Mapeamento das Classes de Serviços			**Tabelas**		
			A	**B**	**C**
Tráfego de Voz		Classe EF	15%	15%	15%
Tráfego de Imagem		Classe AF4	15%	10%	10%
Tráfego de Dados	Alta	Classe AF3	30%	36%	36%
	Média	Classe AF2	14%	15%	15%
	Baixa	Classe AF1	10%	15%	15%
Best Effort			12%	5%	5%
TOTAL			96%	96%	96%

10.9.2 A referida associação trata-se de um exemplo e poderá sofrer alteração na fase de implementação em caráter inicial e não definitivo, cabendo a realização de alterações (sem ônus para o Banco) após a implantação e respectiva avaliação pelo Banco de que tal associação atende ao perfil de tráfego presente na rede.

10.9.3 Respeitando o valor máximo de reserva de 96%, a divisão entre as classes deverá ser composta por números inteiros sem a obrigatoriedade de serem múltiplos de 2 ou 5.

10.9.4 No caso da quantidade de tráfego exceder o reservado para cada classe, deverá ser possível o transbordo de tráfego entre classes, da maior para a de menor prioridade, onde o tráfego excedente da classe AF31, por exemplo, poderá ser remarcado como AF13, a ser definido pelo Banco durante implantação.

10.9.5 As informações referentes aos serviços (IP/porta/protocolo), que deverão ser associados a cada mapeamento das Classes de Serviços, serão repassadas ao início da implantação e ao longo da vigência contratual ao CONTRATADO ITEM 2, que deverá realizar as

marcações apropriadas afim que de as operadoras respeitem em seus respectivos backbones os percentuais; podendo ser alteradas em virtude de novas aplicações/serviços, definições de negócios, melhorias na segurança da informação ou outro critério apontado pelo Banco.

10.9.6 O CONTRATADA **do ITEM 1** receberá o tráfego devidamente marcado nas interfaces dos seus CPEs, seja pelas soluções já existentes no Banco de vídeo e voz, seja pela solução SD-WAN.

10.9.7 Além da operadora ter de manter e priorizar a marcação recebida pela conexão de rede LAN, normalmente com origem do equipamento de SD-WAN, a operadora de MPLS em cada unidade distribuída terá uma lista básica de marcação com base em IP, protocolo e Porta para classificar/marcar. Essa lista poderá igualmente sofrer alterações durante o Contrato. Uma vez que mesmo na indisponibilidade da solução SD-WAN, o tráfego continuará sendo mantido pelo circuito MPLS remanescente, devendo este, pois, utilizar a marcação de QoS contida na lista.

10.9.8 Os percentuais de banda reservados para cada aplicação, dentro das classes de serviço, poderão ser objeto de ajustes durante o prazo contratual, de acordo com as tabelas acima definidas, sem ônus para o Banco. A solicitação de alteração poderá ser feita por unidade remota ou por tipo de link MPLS e deverá respeitar o SLA de configuração.

10.10 Tráfego de gerência para a solução SD-WAN

10.10.1 O tráfego gerado entre a solução de gerenciamento no Site Primário e Site Secundário (definido no **Anexo X - Requisitos de Gerenciamento dos Serviços**) e os equipamentos que serão monitorados deverá ser classificado como pertencente ao tráfego de dados de média prioridade.

10.10.2 A critério do Banco, a prioridade deste tráfego pode ser alterada, após implementação e respectiva avaliação, sem ônus para o Banco.

10.11 Topologia da solução

10.11.1 Deverá ser fornecido desenho esquemático ilustrando todos os aspectos dos requisitos de conectividade, tanto para as unidades distribuídas, postos de crédito quanto para Parceiros como para o Site Primário e Site Secundário. Através deste desenho deverá ser possível identificar a topologia projetada para as redes WAN e LAN, visualizando detalhes sobre as respectivas concentrações, para todos os circuitos.

10.11.2 A arquitetura da rede de comunicações ofertada deverá ser modular, possibilitando escalonar a contratação de aumentos de velocidade para cada um dos circuitos contratados, conforme necessidades futuras do Banco, permitindo ampla flexibilidade de reconfiguração.

10.11.3 As portas e circuitos de acesso deverão permitir aumento de largura de banda de acordo com a demanda futura do Banco, de modo que, quando solicitado pelo Banco, a CONTRATADA procederá a reconfiguração e ativação da nova largura de banda, incluindo os respectivos custos envolvidos nas faturas mensais.

11 REQUISITOS DE SEGURANÇA

Caberá ao Banco estabelecer as políticas de segurança a serem aplicadas aos serviços de telecomunicações CONTRATADAs, equipamentos roteadores e appliances de SD-WAN que compõe a solução e estarão localizados nas dependências do Banco. O Banco terá o direito de verificar a correta aplicação dessas políticas, através da realização de auditorias realizadas a seu

critério, de forma remota, dos equipamentos que compõe a solução. Para garantir os níveis de segurança esperados na infraestrutura por onde trafegarão as informações do Banco, os provedores deverão atender, no mínimo, aos seguintes requisitos:

11.1.1 O CONTRATADA para prover qualquer circuito MPLS deverá prover uma rede IP logicamente independente e isolada de qualquer outra rede, em especial do ambiente público da Internet. O mecanismo para implementar o isolamento e a qualidade de serviços é o MPLS/VPN. Essa garantia deverá ser implementada “fim-a-fim”;

11.11.2 Aplicar em suas redes, para os equipamentos instalados no CAPGV, parceiros, postos e unidades distribuídas, a política de segurança definida pelo Banco para os serviços de telecomunicações, como por exemplo a política atual do Banco que proíbe todo e qualquer acesso de gerenciamento aos equipamentos roteadores via telnet, sendo no mínimo exigido acesso via SSH;

11.11.3 Restringir as informações de segurança a uma equipe restrita de técnicos de segurança, assumindo toda responsabilidade por perdas e danos comprovados que o Banco venha a sofrer em decorrência de dolo, negligência, imperícia ou imprudência dos componentes dessa equipe;

11.11.4 O licitante deverá manter o software dos equipamentos roteadores e/ou appliances atualizados e aplicar tempestivamente correções de vulnerabilidades de segurança publicadas pelo fornecedor, que sejam julgadas importantes pelo Banco;

11.11.5 Para os circuitos de comunicação MPLS, e conforme já especificado nesse anexo, deverá ser fornecido usuário local para acesso via SSH com permissão somente de leitura visando a verificação de configurações e acompanhamento de resolução de incidente. Todas as configurações dos equipamentos deverão ser visíveis por esse usuário fornecido durante todo o Contrato. Para os links de Internet Determinística e internet assimétrica o acesso poderá ser SSH ou HTTPS, ou ambos se for implementando pelo roteador.

12 GLOSSÁRIO

Unidades Distribuídas: Agências, Centrais Operacionais (CENOPs), Unidades de Recuperação de Crédito, Superintendências e demais unidades administrativas do Banco residindo fora do CAPGV;

Parceiros: Entidades parceiras do Banco do Nordeste, responsáveis pela troca de informações bancárias de conteúdo restrito para realização de negócios;

Postos de Crédito: unidades responsáveis pela operacionalização dos produtos de microcrédito (Postos Crediamigo) e crédito rural (Postos Agroamigo) do Banco.

CAPGV: Centro Administrativo Presidente Getúlio Vargas. Sede principal do Banco, onde reside sua administração superior;

Site Primário: Sede primária do Banco, onde residem os principais recursos e serviços centralizados de infraestrutura;

Site Secundário: Sede secundária do Banco, onde reside a redundância dos principais recursos e serviços centralizados de infraestrutura;

Circuito de acesso terciário: conjunto de trechos contínuos de meios de comunicação, completamente independentes daqueles utilizados pelos circuitos de acesso primários e secundários, isto é, sem que haja compartilhamento de qualquer tipo de recurso, exceto em casos onde for fisicamente impossível, o qual interliga uma unidade distribuída, Site Secundário ou o CAPGV a um ponto de presença do fornecedor dos serviços. Usado para balanceamento, contingenciamento do tráfego de dados em caso de falha dos circuitos de acesso primário e secundário, ou para determinados tráfegos escolhidos pelo Banco e roteados na solução SD-WAN;

Circuito de acesso Posto: conjunto de trechos contínuos de meios de comunicação que interliga o posto de crédito a um ponto de presença do fornecedor dos serviços. Usado para tráfego integrado de dados, voz e imagens;

Controle do tráfego: aplicação de mecanismos de identificação, classificação, restrição, filtragem, priorização, ou qualquer outro mecanismo relacionado, sobre fluxos de dados, voz ou imagens;

Ponto de presença: instalações físicas administradas e mantidas pelo fornecedor dos serviços, às quais estão interligados seus diversos clientes. Local onde estão instalados e em operação os equipamentos que compõem o *backbone* do fornecedor dos serviços;

Backbone: conjunto de meios de comunicação e equipamentos, geralmente de alta capacidade de tráfego, usados para interligar os diversos pontos de presença do fornecedor dos serviços;

Ponto de concentração: armário de fiação (*rack*) ou quadro instalado em parede no qual se concentra a terminação do cabeamento horizontal de cada pavimento ocupado por qualquer parte de uma unidade distribuída;

SD-WAN (*Software Defined* – WAN): rede de longa distância definida por software. Cuja solução ora contratada terá a capacidade de determinar os melhores caminhos e rotas para o trafego integrado de dados, voz e imagens entre os Sites Primário e Secundário e as Unidades Distribuídas;

SSE (*Security Service EDGE*): Solução de Gateway de Web Segura de Próxima Geração (NG-SWG) que será responsável pelos serviços de proxy remoto para todas as unidades.

SASE (*Secure Access Service EDGE*): Conceito empregado para a solução completa que engloba SD-WAN e SSE.

NGFW: Solução de Sistemas de firewall de próxima geração.

UTM: Sistemas gerenciamento unificado de ameaças.

NOC/SOC SASE: Centro(s) de Operação(es) de Rede do BANCO e/ou equipe(s) responsável(is) pelo gerenciamento, implementação, correção e controle de toda a solução SD-WAN atual, solução SASE futura, monitoramento dos componentes ofertados pelo **ITEM 1**.

NOC/SOC da Contratada: Centro de Operação de Rede e Segurança responsável pelo gerenciamento, configuração, implementação, suporte, assistência técnica, correção, gerenciamento de SLA e controle de toda a solução, incluindo ajustes de configuração, roteamento, engenharia de tráfego, aplicações de QoS, de funcionalidades de Segurança e demais ajustes necessários da solução ofertada.

Appliance: dispositivo de hardware separado e dedicado com *software* integrado (*firmware*), especificamente projetado para fornecer um serviço específico.

CPE: *Customer Premises Equipment* – Qualquer equipamento instalado nas dependências da Unidade, com a finalidade de conectar e compatibilizar a WAN com a rede local.